



# EU AI Act: Issues and Impacts for HR Leaders



# EU AI ACT: ISSUES AND IMPACTS FOR HR LEADERS

The European Union’s AI Act is currently the world’s most comprehensive legal framework regulating artificial intelligence. With its risk-based approach and broad scope, the Act attempts to ensure the safe and ethical development and deployment of AI technologies used in the EU. Despite fears that it might stifle innovation, the reality is far less dramatic—but also far from trivial.

Often, regulation of any new technology can be viewed as prohibitive—effectively regulating something out of existence. The laundry list of “prohibited” activities in the EU AI Act could be seen as evidence of this. In fact, the current US administration has tried to counter that perception by pulling back on the prior administration’s attempt to regulate AI. The current administration even tried to prevent the various states from regulating AI as a result of this “regulate out of existence” perception. This seems to create tension between the EU approach and the US approach to AI regulation.

## A. Spoiler Alert: AI Is Not Banned

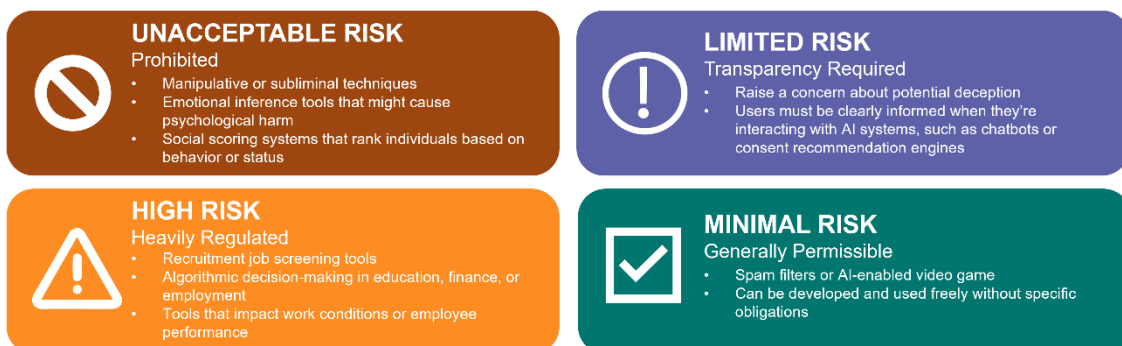
Let’s set the record straight—AI is not being banned in Europe. The intention of EU AI Act is not to smother innovation but rather to shape it in a manner aligned with the interests of the EU member states. Development and deployment of AI are still very much on the table—but they must now be undertaken in a thoughtful, transparent, and compliant manner with clearly defined standards. But as with any sweeping regulation, tension is inevitable, particularly around interpreting vague risk definitions and adapting HR practices to meet formal regulatory scrutiny.

Additionally, since the EU AI Act is a “first mover” in the space of comprehensive regulation, it is not unexpected to see a number of other jurisdictions take up the EU’s approach. In fact, despite the US federal government’s focus on deregulation, as well as the federal government’s failed efforts to pass a moratorium on state regulation, the State of Colorado has passed a law which is remarkably similar to the EU AI Act. California and other states may not be far behind. Companies operating both in Europe and in the United States, particularly those with multistate US operations, should be planning now for the EU AI Act’s requirements and pay close attention to the inevitable emergence of a patchwork of US state regulations as they continue to make transformative investments in artificial intelligence—not just in human resources (which is the focus of this article) but throughout the organization.

## B. Understanding the Regulatory Landscape

At its core, the EU AI Act employs a risk-based classification that categorizes AI systems from “minimal” risk to those that are “unacceptable.” At the heart of the EU AI Act is the classification of AI systems by risk levels:

### AI Risk Management – Risk Levels



## **1. Unacceptable Risk—Prohibited**

Systems with “unacceptable risk” are outright banned. They typically involve:

- Manipulative or subliminal techniques
- Emotional inference tools that might cause psychological harm
- Social scoring systems that rank individuals based on behavior or status

The banning of “social scoring systems” is particularly noteworthy. The EU AI Act aims to prevent AI systems from evaluating things like online purchases, social media activity, and sentiment analysis to create scores or rankings that would be used to determine eligibility for loans, set insurance rates, or receive other services.

## **2. High Risk—Heavily Regulated**

“High risk” systems are permitted but must meet stringent requirements. Common examples include:

- Recruitment and job screening tools
- Algorithmic decision-making in education, finance, or employment
- Tools that impact work conditions or employee performance

For HR practitioners, based on the categorization of many HR AI use cases as “high risk,” the EU AI Act requires evaluation of everything from automated candidate screening tools to AI-enhanced performance evaluations through a rigorous risk lens. Any system deemed “high-risk” must undergo comprehensive internal checks, adhere to strict documentation protocols, and be subject to continuous human oversight.

In addition, HR practitioners should consider whether actual or potential future applications of AI in human resources functions even could be characterized as “unacceptable risk” and prohibited outright. For example, when evaluating applicants who are scored or ranked based on what they say during an interview is presumably high risk, what about scoring or ranking systems based on AI-analyzed candidate “behavior” during an interview? What about AI tools that would seek to evaluate, rank, or score employees based on analyses of employee engagement or sentiment derived from work communications?

Failure to understand or comply with EU AI Act requirements could expose organizations to significant legal and financial liabilities.

## **3. Limited Risk—Transparency Required**

Systems that pose “limited risk” are those that raise a concern about potential deception. Users must be clearly informed when they’re interacting with AI systems, such as chatbots or content recommendation engines.

#### **4. Minimal Risk—Generally Permissible**

“Minimal risk” systems—like spam filters or AI-enabled video games—can be developed and used freely without specific obligations.

### **C. Scope of Impact on HR Systems**

A closer look at the Act reveals a sweeping definition of what constitutes AI. Beyond high-profile technologies like chatbots and conversational AI, traditional HR systems—often embedded with algorithmic decision-making—can no longer be viewed as benign tools.

Companies and their HR professionals are now tasked with ensuring that even familiar processes, such as digital talent management systems or cloud-based HR applications, meet the elevated standards imposed by the Act. The EU AI Act casts a wide net over what qualifies as “artificial intelligence.” The concept of AI in the Act is not limited to large language models (LLMs) or chatbots. The Act applies to:

- Machine learning systems
- Knowledge-based systems
- Statistical or algorithmic tools
- Systems that influence physical or digital environments through predictions, recommendations, or decisions

This includes background screening, performance evaluation tools, and virtually any software that adapts over time.

### **D. Compliance Challenges in High-Stakes HR Procedures**

For HR functions that significantly impact employee lives—such as recruitment and career development—the compliance checklist can be particularly demanding. The Act calls for implementing detailed risk management procedures akin to those found in industries like medical devices. HR departments are advised to institute comprehensive risk assessments, continuous performance testing, and transparent communication channels with employees. Regular training and updated protocol reviews are essential to keep pace with evolving regulatory expectations.

Taking the EU General Data Protection Regulation as an analogy (particularly since the GDPR has many of the requirements for “accountability mechanisms” that the EU AI Act does), compliance program development, implementation, and management will require some significant resources—in both legal and operational areas.

For example, policies will need to be drafted articulating what kinds of AI can be used for what kinds of purposes. Risk assessment tools will need to be created to identify and measure legal risks as articulated by the AI Act. Standards will need to be drafted relating to when and how bias audits, risk assessments, use case approvals, and similar tactical decisions are made for the purpose of deploying AI. Standards around performance testing will need to be drafted. Training will need to be created, deployed, and evaluated for effectiveness.

All of the above will need significant input (if not primary effort in creation) from legal counsel who are fluent in the requirements of the EU AI Act.

## **Use Case: The Role of AI in Talent Acquisition: Benefits and Challenges**

AI has become a powerful tool in the talent acquisition process, helping HR professionals streamline recruitment, improve candidate screening, and make data-driven hiring decisions. From automating resume parsing to conducting initial interviews through chatbots, AI is now integral to modern recruitment strategies. However, with these advancements come significant responsibilities, especially under the EU AI Act, which mandates high standards for AI systems in high-risk areas like hiring and employment.

In talent acquisition, AI is used across several stages of the hiring process:

- **Resume Screening and Candidate Sourcing**

AI-powered systems can scan hundreds or thousands of resumes to automatically filter and rank candidates based on specific criteria, such as qualifications, skills, and experience. These tools often use natural language processing (NLP) and machine learning algorithms to analyze resumes, match job descriptions, and recommend candidates who are most likely to succeed in the role.

- **Predictive Analytics for Candidate Success**

Some AI tools use predictive analytics to evaluate a candidate's potential fit for a role or organization. By analyzing historical data—such as previous employee performance, tenure, and success rates—these systems can predict how well a new candidate might perform, even before they've been hired.

- **Chatbots and Virtual Interviews**

AI-powered chatbots are increasingly being used for initial candidate engagement. These bots can conduct preliminary screenings, answer candidate questions, and even schedule interviews. Some systems even offer virtual interview platforms that evaluate candidates' responses using speech and facial recognition technologies to assess personality traits or cognitive abilities. The last use case brings in the specter of “emotional inference” processing, which is prohibited by the EU AI Act.

- **Bias Detection Tools**

AI can also help identify and mitigate unconscious bias in the recruitment process. By using data-driven algorithms, AI can ensure that the criteria for shortlisting candidates are based on objective factors, reducing the risk of biases related to gender, race, or background.

The AI Act places HR departments under the spotlight when it comes to the use of AI systems in hiring. Specifically, AI systems used in talent acquisition are considered high-risk due to the potential impact they have on individuals' livelihoods and rights.

So—what should HR teams do to take advantage of the capabilities of AI in the Talent Acquisition space?

## E. Components of a Risk Management Program for AI Use in HR

### 1. Governance and Accountability

Developing a strong governance framework is essential for AI risk management, ensuring accountability, and making sure that compliance requirements are met. This is critical throughout the organization and applies to any use of AI, not just the use of AI in HR functions, and many organizations may well have AI governance frameworks already in place that are focused on more customer-facing AI analyses (such as marketing, supply chain management, logistics, etc.). However, many HR leaders may be surprised to learn that the HR systems they are seeking to revolutionize—as well as the many vendors flooding the market to push those solutions—will be subjected to considerable scrutiny under the EU AI Act and emerging state laws. Organizations must be prepared to sweep up HR AI use cases into their existing governance framework, and start adapting the framework through an HR lens.

#### Key Actions:

(a) **Assign Clear Responsibility:** Designate an AI ethics officer, compliance officer, or AI risk management team within the HR department. This team should have a cross-functional composition, including IT, data privacy experts, and legal advisors.

(b) **Define Roles and Responsibilities:** Ensure that all stakeholders, from developers to deployers, understand their roles in managing AI-related risks. Developers are responsible for creating AI models that are ethical and compliant, while HR deployers are responsible for proper implementation and ongoing oversight.

(c) **Establish AI Governance Policies:** Develop policies that cover: how AI systems should be used in HR activities, detailing decision-making processes, criteria for risk assessment, and compliance obligations. These policies should also define the scope of AI applications, especially regarding sensitive HR processes like recruitment, performance evaluation, and promotion decisions.

### 2. Risk Identification

The first step in managing risk is understanding what risks exist. HR professionals must identify risks that could potentially harm candidates, employees, or the organization. AI systems used in HR often involve personal data, bias, discrimination, and transparency issues, so these need to be closely examined.

#### Key Actions:

(a) **Identify AI System Components:** List the AI tools used in HR processes, such as applicant tracking systems (ATS), resume parsing algorithms, candidate assessment tools, and AI-powered performance management systems.

(b) **Assess Potential Risks:** Evaluate the specific risks each AI system could introduce:

(i) **Bias and Discrimination:** AI models trained on biased data can perpetuate unfair treatment based on gender, age, race, or disability status.

(ii) **Privacy Violations:** AI tools that analyze personal data (e.g., resumes, interview recordings) must comply with data protection laws like GDPR. Data breaches or misuse can lead to reputational damage and legal consequences.

(iii) **Lack of Transparency:** If AI tools make decisions that affect employees or candidates without clear explanations, this could lead to mistrust and legal challenges.

(iv) **Over-reliance on AI:** Depending too heavily on AI could reduce human judgment in critical HR decisions, potentially missing nuances in candidate assessment or employee development.

(c) **Engage Stakeholders:** Work with legal, compliance, and diversity teams to help identify potential legal, ethical, and social risks. This collaborative effort ensures a broad perspective on the potential risks AI poses in HR.

### 3. Risk Assessment and Evaluation

Once the risks have been identified, the next step is to assess their impact and likelihood.<sup>1</sup> In this phase, HR professionals must evaluate the severity of each risk and determine which ones require immediate action.

#### Key Actions:

(a) **Risk Matrix:** Use a risk matrix (e.g., high, medium, low) to assess the likelihood and impact of each identified risk. This helps prioritize which risks should be mitigated first.

(i) **High-Likelihood, High-Impact Risks:** These are the risks that need immediate attention and robust mitigation strategies (e.g., bias in recruitment algorithms).

(ii) **Low-Likelihood, High-Impact Risks:** These require contingency planning and monitoring, even if they are less likely to occur (e.g., data breaches).

(b) **Impact on Stakeholders:** Consider the potential harm to stakeholders, including candidates, employees, and the organization. Risks like biased hiring processes or privacy violations can have serious legal and reputational consequences.<sup>2</sup>

(c) **Regulatory Requirements:** Ensure that your risk assessment incorporates compliance with the EU AI Act, GDPR, and other relevant legislation. Evaluate whether the AI systems used in HR meet the requirements for high-risk AI systems under the EU AI Act. In the United States, evaluate whether you're complying with the more stringent auditing requirements of New York City, Colorado and California, as well as the notification and other requirements of Illinois.

---

<sup>1</sup> EU AI Act penalties follow a similar pattern as GDPR. However, they are actually larger at the top end. Violations of the EU AI Act can result in administrative penalties in the amount of 7% of a business' gross annual revenue, or €35,000,000, whichever is higher. EU AI Act Article 99(3).

<sup>2</sup> *Id.*

## 4. Risk Mitigation

Once risks have been assessed, HR must develop and implement strategies to mitigate them. This includes both technical solutions (such as algorithm adjustments) and organizational measures (such as training and oversight).

### Key Actions:

(a) **Bias Mitigation:** Implement bias detection tools and regularly audit AI models to ensure they do not perpetuate discriminatory practices. This could involve:

- Using diverse datasets for training AI models to ensure they reflect a wide range of candidates.
- Testing AI outputs for fairness and adjusting models based on the results, to ensure that analyses do not disproportionately affect protected groups. This may require the use of third-party experts, law firms, I/O psychologists or other professionals to conduct demonstrable anti-bias testing in places like New York and Colorado, as well as the EU.

(b) **Transparency Mechanisms:** Ensure that AI systems are transparent and that candidates and employees can understand the decisions made by AI tools. Some actions HR can take include:

- Providing clear explanations of how AI tools assess candidates or workers and the decision criteria.
- Providing opt-out options for individuals who prefer human interaction over AI-driven processes (e.g., offering a human review for automated resume screening).

(c) **Data Protection:** Ensure AI systems comply with GDPR and other data protection laws by:

- Minimizing the data collected and only using personal data necessary for the decision-making process.
- Implementing encryption and access control measures to protect sensitive employee and candidate data.
- Performing Data Protection Impact Assessments (DPIAs) for AI systems that process personal data.

(d) **Human Oversight:** Implement policies that ensure human oversight of AI decisions in critical HR processes. This could include:

- Ensuring that automated decisions (like shortlisting candidates) are reviewed by HR personnel to ensure fairness.

- Allowing employees and candidates to appeal AI-driven decisions or request a human review.
- Employee and Candidate Training: Train HR professionals and employees on how to use AI tools effectively and ethically. This training should include:
  - Recognizing and correcting AI bias in recruitment processes.
  - Understanding the limitations of AI tools (e.g., predictive hiring tools can't fully replace human discretion).
  - Training on data protection principles, especially related to sensitive employee and candidate data.

## 5. Monitoring and Continuous Improvement

An effective risk management program doesn't stop at mitigation—it requires ongoing monitoring and adjustment to ensure that AI systems continue to operate fairly and effectively. Regular audits and feedback loops are key to this process.

### Key Actions:

(a) **Continuous Monitoring:** HR should regularly monitor AI-driven hiring processes to ensure that they're working as expected. For example:

- Conduct periodic audits of AI systems to ensure they remain free of bias.
- Track and evaluate recruitment outcomes, paying close attention to whether AI systems are disproportionately selecting or rejecting candidates from particular demographics.

(b) **Feedback Mechanisms:** Implement feedback mechanisms to collect input from employees, candidates, and hiring managers. This could include:

- Surveys or interviews with candidates to assess their experience with AI-driven processes.
- Gathering HR staff feedback on how AI tools affect their workflow and hiring decisions.

(c) **Corrective Actions:** Based on monitoring and feedback, HR must be prepared to implement corrective actions if any issues or risks are identified. This might involve:

- Adjusting AI models or retraining them using updated, more diverse datasets.
- Revising policies or procedures to address emerging risks or compliance concerns.

(d) **Regular Training and Updates:** As AI technologies and regulations evolve, HR professionals must stay updated on new best practices and legal requirements. This can be done through:

- Ongoing training on emerging AI trends, risks, and regulations.
- Keeping abreast of updates to the EU AI Act and other relevant legislation.

## 6. Documentation and Reporting

Under the EU AI Act, HR professionals must ensure that all AI systems used in recruitment and other HR processes are properly documented and subject to conformity assessments.

### Key Actions:

(a) **Maintain Detailed Records:** HR must maintain thorough documentation of the AI systems used in the recruitment process, including:

- AI system description (how it works, what data it uses, etc.)
- Risk assessment and mitigation strategies (this includes Fundamental Rights Impact Assessments, or “FRIAs”).
- Audit and monitoring results.

(b) **Conformity Assessment Reports:** Ensure that the AI systems used in HR are subject to regular conformity assessments (since, by statute under EU law, all HR-related use of AI is “High Risk”) to confirm that they meet the standards outlined in the EU AI Act.

(c) **Incident Reporting:** Establish protocols for reporting significant incidents (e.g., discrimination, data breaches) that may arise from the use of AI systems.

## F. HR Risk and Vendor Management Accountability

One of the more challenging aspects for HR departments, and the procurement departments that support them, is the new power dynamic along the AI supply chain. The regulation goes beyond the end-user: providers, third-party vendors and even sub-suppliers must comply with the new regulatory framework. As such, HR leaders must collaborate closely with internal IT, procurement, and legal teams to implement robust vendor management practices and ensure that every technological element within their HR ecosystem is compliant. The Act addresses the entire AI supply chain, not just core developers. The regulated players include:

- Providers—Those who create systems containing AI
- Sub-suppliers—Developers of the underlying AI components
- Importers/Distributors—Those who place AI on the EU market
- Deployers—Organizations or individuals who use the AI in practice

Even SaaS platforms embedding AI fall under the regulation if they are marketed in or deployed within the EU.

## **G. Strategic and Ethical Imperatives**

While regulatory compliance is paramount, the EU AI Act also serves as a clarion call for HR professionals to re-examine the strategic and ethical dimensions of AI adoption. On one hand, AI holds the promise of impartially optimizing talent management and reducing human biases. On the other, unchecked automation risks embedding subtle psychological and emotional challenges into the workplace. HR teams must, therefore, craft policies that not only adhere to legal requirements but also reinforce principles of fairness, transparency, and respect for employee dignity.

## **H. Transforming Compliance Into a Competitive Advantage**

The EU AI Act should not be seen only as a constraint, but also as an opportunity for HR innovation. By proactively aligning AI tools with regulatory standards, HR departments can lead the change in defining an ethical, efficient, and compliant workforce of the future. It is now time to develop robust internal guidelines, vet technology partners meticulously, and engage in continuous dialogue with legal experts to pre-emptively address regulatory shifts.

In conclusion, as businesses throughout Europe brace for the ripple effects of the EU AI Act, HR professionals are uniquely positioned to turn new challenges into strategic advantages. By marrying legal compliance with ethical oversight, HR departments can play a critical role in steering companies towards an AI-enabled future where technology enhances human potential without compromising on accountability.