FIRM
Frankfurter Institut für
Risikomanagement und Regulierung

Regulierung von KI im Personalbereich: Anforderungen, Risiken und Umsetzung

Autoren
Ihno Raab

Mit dem AI Act liegt erstmals ein europaweit einheitlicher, rechtsverbindlicher Rahmen für den Einsatz von Künstlicher Intelligenz [EU 2024] vor. Für HR-Abteilungen bedeutet dies einen Paradigmenwechsel: Was bisher als Innovationsprojekt galt, wird nun auch zum Compliance-Thema. Systeme zur Bewerberauswahl, Leistungsbewertung oder Personalplanung werden als "Hochrisiko-KI" eingestuft - mit weitreichenden Konsequenzen für Governance, Dokumentation und Kontrolle.

Die regulatorische Uhr tickt: Ab August 2026 greift der AI Act für neue HR-Systeme. Bestehende Systeme müssen bei wesentlichen Änderungen nachgerüstet werden. Doch zwischen Gesetzestext und Unternehmensrealität klafft eine Lücke: Wie lassen sich diese Vorgaben in heterogenen Tool-Landschaften, mit SaaS-Anbietern und unter Einbindung von HR-Mitarbeitern und Betriebsräten tatsächlich umsetzen? Dieser Beitrag analysiert zentrale Umsetzungsrisiken und zeigt Lösungswege auf.

Einordnung: Was fällt unter Hochrisiko-KI?

Der AI Act unterscheidet KI-Systeme nach Risikostufen. Besonders relevant für HR ist Anhang III, der Systeme zur Personalbeschaffung, -auswahl, -bewertung, -förderung und Systeme zur Beendigung von Vertragsverhältnissen als Hochrisiko-Systeme einstuft [EU 2024, Anhang III]. Entscheidend ist dabei nicht die Technologie, sondern der Wirkungsgrad: Auch vermeintlich harmlose Tools wie CV-Screening-Software oder automatisierte Skill-Matching-Systeme fallen darunter, wenn sie Entscheidungen beeinflussen.

Praxisbeispiel: Ein Unternehmen nutzt ein KI-gestütztes Recruiting-Tool, das Bewerbungen vorfiltert. Nutzt der Recruiter diese Vorauswahl als Grundlage seiner Entscheidung, ist das System hochrisikobehaftet - selbst wenn formal "ein Mensch entscheidet". Die Abgrenzung zwischen "Entscheidungsunterstützung" und "hochrisikobehafteter Einflussnahme" bleibt in der Praxis oft unklar und erfordert eine Einzelfallprüfung.

Wo Regulatorik auf Unternehmensrealität trifft

Die regulatorischen Anforderungen steigern die Komplexität der Umsetzung:

Konformitätsprüfung: Jedes Hochrisiko-System muss vor Inbetriebnahme geprüft werden - eine Aufgabe, für die weder HR noch IT typischerweise ausgestattet sind.

Menschliche Aufsicht: Die geforderte Aufsicht bleibt vage. Wie kann diese bei 500 automatisierten CV-Screenings pro Tag praktisch gestaltet werden?

Transparenzpflicht: Mitarbeitende müssen "in verständlicher Sprache" über KI-Einsatz informiert werden - eine Gratwanderung zwischen rechtlicher Präzision und Verständlichkeit.

Technische Dokumentation: Bei SaaS-Lösungen mit KI-Modellen bleiben Trainingsdaten und Modelllogik oft proprietär. Das Anwenderunternehmen ist dennoch rechenschaftspflichtig - mit unvollständigen Informationen.

Diese Anforderungen sind primär organisatorisch herausfordernd, nicht technisch. Die eigentliche Schwierigkeit liegt in der funktionsübergreifenden Koordination zwischen HR, IT, Datenschutz, Recht und Betriebsrat.

Vendor-Management: Verantwortung bleibt beim Anwender

Die meisten HR-Systeme werden nicht intern entwickelt, sondern als SaaS-Dienste eingekauft. Die Verantwortung bleibt dennoch beim anwendenden Unternehmen - unabhängig davon, wer das System entwickelt hat. Dabei sind besonders folgende Aspekte zu beachten:

Vertragsgestaltung: Lieferverträge müssen explizit regeln, wer für Konformitätsprüfung, Dokumentation und laufendes Monitoring verantwortlich ist. Standardverträge müssen hier sorgsam geprüft werden.

Due Diligence: Vor Einführung eines Systems sollten Anbieter Nachweise liefern: CE-Kennzeichnung, technische Dokumentation, Bias-Prüfverfahren und implementiertes Risikomanagement-System.

Laufende Überwachung: Auch nach Implementierung müssen Systeme regelmäßig überprüft werden - etwa bei Modellupdates oder Änderungen der Nutzungsweise. Dies erfordert Eskalationswege und Prüfzyklen.

Betriebsrat und Mitbestimmung: Die unterschätzte Dimension

Der AI Act trifft in Deutschland auf ein etabliertes System der betrieblichen Mitbestimmung. §87 Abs. 1 Nr. 6 BetrVG räumt Betriebsräten ein Mitbestimmungsrecht bei technischen Einrichtungen ein, die zur Verhaltens- oder Leistungsüberwachung geeignet sind [BetrVG] - eine Beschreibung, die auf viele KI-Systeme im Personalwesen zutrifft.

AI Act und BetrVG verfolgen unterschiedliche Logiken: Selbst ein AI-Act-konformes System kann an fehlender Betriebsratszustimmung scheitern.

Folgende Ansätze haben sich bewährt

Frühzeitige Transparenz: Betriebsräte sollten bereits in der Planungsphase informiert werden - nicht erst bei Inbetriebnahme. Je früher die Einbindung, desto geringer das Konfliktpotenzial.

Verständliche Kommunikation: Technische Dokumentation allein genügt nicht. Betriebsräte benötigen verständliche Erläuterungen zu Funktionsweise, Datenverwendung und möglichen Auswirkungen auf Beschäftigte.

Klare Verantwortlichkeiten: Betriebsvereinbarungen sollten regeln, wer bei Problemen oder Beschwerden Ansprechpartner ist und wie Korrekturen eingeleitet werden.

Pilotphasen und Evaluation: Betriebsräte sind eher bereit, neuen Systemen zuzustimmen, wenn diese zunächst in begrenztem Umfang getestet und evaluiert werden.

Unternehmen, die Betriebsräte als Partner statt als Hindernis begreifen, schaffen Rechtssicherheit und stärken zugleich Akzeptanz bei der Belegschaft - ein entscheidender Faktor für nachhaltige KI-Einführung.

Ein Umsetzungsansatz in vier Schritten

Schritt 1 - Bestandsaufnahme und Klassifikation: Erfassung aller eingesetzten KI-Tools im HR-Bereich, inklusive SaaS-Lösungen und Eigenentwicklungen. Dokumentation von Anbieter, Funktionsumfang und Entscheidungstiefe. Anschließende Bewertung anhand der AI-Act-Kriterien mit einer Risikomatrix (Automatisierungsgrad x Auswirkung auf Mitarbeitende).

Schritt 2 - Gap-Analyse: Abgleich zwischen regulatorischen Anforderungen und aktuellem Status. Wo fehlen Dokumentationen? Wo sind Vendor-Informationen lückenhaft?

Schritt 3 - Rollen- und Prozessmodell: Definition klarer Verantwortlichkeiten. Wer führt Konformitätsprüfungen durch? Wer überwacht laufende Systeme? Wer kommuniziert mit Betriebsrat und Datenschutz? Ein RACI-Modell (Responsible, Accountable, Consulted, Informed) schafft Klarheit.

Schritt 4 - Integration in Bestehendes: Anbindung an vorhandene Compliance-Strukturen (z. B. Datenschutz-Management, IT-Risikomanagement). Dabei etablierte Prozesse nutzen, so können etwa Datenschutz-Folgenabschätzungen und AI-Act-Dokumentation teilweise zusammengeführt werden.

Unternehmen, die frühzeitig handeln, sichern Compliance und schaffen Wettbewerbsvorteile. KI-Compliance wird zunehmend relevant für Ausschreibungen, ESG-Ratings.

Fazit

Mit dem AI Act wird der Einsatz von KI-Systemen im Personalbereich umfassend reguliert. Die Herausforderung liegt nicht im Verstehen der Anforderungen, sondern in ihrer Umsetzung - insbesondere an den Schnittstellen zwischen HR, IT, Recht und Betriebsrat.

Entscheidend sind ein Vendor-Management, das Verantwortung klar zuordnet; die aktive Einbindung von Betriebsräten, die regulatorische mit betriebsverfassungsrechtlichen Anforderungen verzahnt; und ein strukturierter Implementierungsfahrplan, der pragmatisch vorgeht und dokumentiert wird.

Unternehmen müssen nicht ab Tag 1 perfekte Systeme vorweisen - aber sie brauchen einen nachvollziehbaren Weg dorthin. In einem zunehmend regulierten Umfeld wird KI-Compliance zum Wettbewerbsvorteil.

Quellen

EU [2024]: Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz), Amtsblatt der Europäischen Union L 2024/1689

BetrVG [1972]: Betriebsverfassungsgesetz in der Fassung der Bekanntmachung vom 25. September 2001 (BGBl. I S. 2518), zuletzt geändert durch Artikel 6 des Gesetzes vom 20. Mai 2020 (BGBl. I S. 1044).

Autor

Ihno Raab

Head of HR Consulting Services

d-fine GmbH, Frankfurt am Main

Scannen für Online-Version
https://firm.fm/?p=10603