COMPLIANCE WORKSHEET

EU AI Act compliance checklist for hiring teams

The EU Council postponed high-risk AI Act obligations to December 2, 2027 — but the penalties (€35M or 7% of global turnover), the high-risk classification of AI hiring tools under Annex III, and your responsibility as the deployer are unchanged. Compliance takes 12–18 months to build properly; bias testing protocols alone need 6 months of data. Work through these 12 points now and refine as the CEN/CENELEC standards crystallise.

How to use it: tick a box only when the evidence exists — a document, a log, a signed contract — not when someone says it is handled. Full context for each point: recruo.com/blog/eu-ai-act-hiring-checklist.

- [ ] **1. Inventory all AI tools used in hiring**

  Catalog everything that processes candidate data and produces a score, ranking or recommendation: ATS, resume parsers and rankers, sourcing tools that score profiles, AI skill assessments, video interview platforms, AI-assisted background checks.

- [ ] **2. Classify each tool against Article 6 (high-risk criteria)**

  Most hiring AI is high-risk under Annex III: recruitment or selection, promotion or termination decisions, task allocation, performance monitoring. Document the classification reasoning for every tool, including the ones you rule out.

- [ ] **3. Risk management process (Article 9)**

  Identify known and reasonably foreseeable risks (bias, discrimination, errors), estimate their impact, adopt mitigations and test that they work. Start with a 1-page risk register per AI tool.

- [ ] **4. Data governance and quality (Article 10)**

  Ask vendors to document training data sources and bias testing on protected characteristics. Run your own output monitoring: do candidates from one group get systematically lower scores than another?

- [ ] **5. Technical documentation (Article 11)**

  Keep the Annex IV pack on file: system description, components and processes, risk management, data governance, cybersecurity measures, performance metrics, human oversight design, lifecycle procedures, conformity assessment.

- [ ] **6. Record-keeping and logging (Article 12)**

  The system must automatically log every candidate evaluation, every human override and every model update. Retain for a minimum of 6 months — ideally 5+ years for hiring decisions, matching the GDPR statute of limitations for discrimination claims.

- [ ] **7. Transparency and information to candidates (Article 13)**

  Tell candidates before AI evaluation begins: that AI is used, what data is processed, what the AI assesses, and that they have the right to a human review. A clear consent screen meets the bar; a clause buried in a privacy policy does not.

- [ ] **8. Human oversight design (Article 14)**

  A human must be able to understand the AI output, override it, and be organisationally empowered to actually do so — with overrides and their rate recorded. A human rubber-stamping AI decisions is not oversight.

- [ ] **9. Accuracy, robustness, cybersecurity (Article 15)**

  Document accuracy metrics (precision, recall, F1) on a representative test set, performance on edge cases such as non-native English speakers, adversarial robustness, and security for data at rest and in transit (vendor SOC 2).

- [ ] **10. Conformity assessment and CE marking**

  Internal control (Annex VI) against a harmonised standard, or third-party assessment (Annex VII) where no standard exists or biometrics are involved. Standards are not final — track CEN/CENELEC progress quarterly.

- [ ] **11. Post-market monitoring**

  Once deployed: monitor model performance drift and bias drift, report incidents where the AI caused harm, and re-assess at least annually.

- [ ] **12. Vendor due diligence**

  Ask every vendor: conformity assessment status, bias testing protocol and latest results, retention and deletion policy, the exact human oversight flow, and the plan for when standards finalise. Fewer than 4 of 5 confident answers is a vendor risk problem.

ACTION PLAN

The first 90 days

By day 90 you will have a compliance foundation that can absorb whatever the final standards look like — without a fire drill.

Window	Focus	What to do
Days 1–30	Audit and inventory	Catalog every AI tool in your hiring stack. Classify each against Article 6. Document the current state: what is logged, who reviews, what is documented.
Days 31–60	Documentation and vendor contracts	Update vendor contracts to include AI Act compliance commitments. Build a risk register for each high-risk tool. Implement candidate notification flows.
Days 61–90	Bias testing and human oversight SOPs	Define and document your human oversight process. Set up bias monitoring on outputs. Train the hiring team on override procedures. Draft the candidate appeals workflow.

Common traps

- "Our vendor said they are compliant" — without CE marking that is a marketing claim. Ask for the documentation, not the claim.
- "We use a US tool, so the Act does not apply" — the Act applies where the AI and its outputs are used, not where the vendor is incorporated.
- "GDPR covers us" — GDPR is about the data; the AI Act is about the system. You need both.

NEXT STEP

Want a second pair of eyes on your compliance posture?

Book a 30-minute compliance review. We will walk through this checklist against your hiring stack and share the templates we use — risk register, candidate notification flow, human oversight SOP. No sales pitch required.

Book a call: calendly.com/odatskiv-recruo/30min
Email: odatskiv@recruo.com
Web: recruo.com