EU AI Act: *Action Items Checklist*

SPRINTO

1. Transparency obligations

due Aug 2

- [ ] List every place where customers, employees, candidates, partners, or users interact with AI
- [ ] Identify AI-generated content in marketing, support, product, training, comms, and public-facing material
- [ ] Check where disclosure is required: chatbots, AI assistants, synthetic content, deepfake utilization if any, biometric or emotion recognition tools, and any text generated by AI
- [ ] Create standard disclosure language
- [ ] Assign an owner for approving, placing, testing, and maintaining disclosures
- [ ] Add disclosure checks to product launches, marketing reviews, vendor intake, and change management

2. Broader AI Act applicability

due Aug 2

- [ ] Build or update an AI inventory
- [ ] Classify AI use cases by business function, owner, vendor, geography, data type, user impact, and risk level
- [ ] Create a simple AI intake process for new tools and features
- [ ] Add AI questions to vendor due diligence
- [ ] Define who approves AI use cases: Legal, Security, Privacy, Product, HR, Compliance, or Procurement
- [ ] Create evidence trails for decisions: why a use case was approved, what disclosures were added, what controls exist, and when it will be reviewed

3. AI literacy

already in force since Feb 2025

- [ ] Identify teams that use or oversee AI: Product, Engineering, Support, HR, Marketing, Sales, Security, Legal, Procurement. Appoint a job title as owner, not a department
- [ ] Create role-based AI training instead of one generic module
- [ ] Cover the basics: hallucinations, sensitive data, human review, bias, confidentiality, customer impact, and escalation
- [ ] Maintain evidence of training completion and updates
- [ ] Add AI literacy to onboarding for relevant roles

4. Prohibited practices

already in force since Feb 2025

- [ ] Screen existing AI use cases for prohibited practices
- [ ] Add a "prohibited use" check to AI intake
- [ ] Create a fast escalation path for questionable use cases
- [ ] Document why each AI use case does not fall into the prohibited bucket
- [ ] Make sure vendors are contractually restricted from using AI in ways that could create prohibited-practice exposure

5. High-risk obligations

expected Dec 2027

- [ ] Identify possible high-risk use cases, especially in HR, finance, education, customer eligibility, infrastructure, safety, and legal workflows
- [ ] Create a high-risk AI register
- [ ] Define required controls per the EU AI Act's guidelines: risk assessment, data governance, documentation, logging, testing, human oversight, monitoring, security, and incident response
- [ ] Decide what evidence will be needed for each control
- [ ] Build a roadmap by maturity level: basic inventory first, then risk classification, then controls and evidence