EU AI Act Compliance Checklist

Enterprise Edition — 2025/2026 Enforcement Timeline

This checklist maps obligations across the four EU AI Act risk tiers. Work through each section with your legal, technical, and risk teams. Tick each item to confirm compliance or flag it for remediation.

PROHIBITED Prohibited AI Practices — Must Not Deploy

- [ ] Identify and audit all AI systems against the Article 5 prohibited practices list.

Prohibited since 2 Feb 2025. Violations carry fines up to €35M or 7% of global turnover.

- [ ] Confirm no AI system uses subliminal or manipulative techniques to distort behaviour.

Includes dark-pattern-style AI nudging targeting vulnerabilities.

- [ ] Confirm no 'social scoring' systems rank individuals based on behaviour or personal characteristics.
- [ ] Confirm no real-time remote biometric identification in publicly accessible spaces (unless law enforcement exception applies).
- [ ] Confirm no AI-based emotion recognition in workplace or educational settings.

Limited exceptions exist — take legal advice before any deployment.

- [ ] Document prohibition assessments and retain for audit.

HIGH-RISK High-Risk AI Systems — Article 10–17 Obligations

- [ ] Perform conformity assessment for each high-risk AI system (Annex III list).

Includes: CV screening, credit scoring, biometric categorisation, critical infrastructure AI.

- [ ] Implement a risk management system documented throughout the AI lifecycle.

Article 9 — must be continuous, not a one-off exercise.

- [ ] Establish and document data governance practices for training, validation, and test data.

Article 10 — bias testing and dataset quality documentation required.

- [ ] Prepare Technical Documentation (Article 11 + Annex IV) before market placement.
- [ ] Implement automatic logging / audit trail for high-risk AI system operations.

Article 12 — logs must enable post-market monitoring.

- [ ] Produce Instructions for Use for deployers (human-readable, Article 13).
- [ ] Implement human oversight measures — identify and assign qualified natural person(s).

Article 14 — oversight must be meaningful, not rubber-stamp.

- [ ] Ensure accuracy, robustness, and cybersecurity standards are met and documented.

Article 15 — include adversarial testing results.

- [ ] Register high-risk AI systems in the EU AI Act database (when operational).

Article 71 — registration obligation applies to providers and certain deployers.

- [ ] Appoint an EU-based authorised representative if the organisation is outside the EU.

TRANSPARENCY — Transparency-Obligation AI Systems — Article 50

- [ ] Identify all chatbots, AI-generated content, and synthetic media tools.

Article 50 in effect — users must know they are interacting with AI.

- [ ] Implement disclosure notices for any AI interacting directly with natural persons.

Chatbots must self-identify as AI at session start.

- [ ] Label AI-generated text, audio, video, and images with machine-readable metadata.

Deep fake / synthetic media — watermarking or equivalent technical measures required.

- [ ] Document transparency measures and review on each product update.

MINIMAL — Minimal-Risk AI Systems — Voluntary Codes of Conduct

- [ ] Categorise all remaining AI systems as minimal-risk and document the rationale.

Retain the classification rationale to justify non-registration.

- [ ] Consider voluntary adherence to applicable Codes of Conduct (Article 95).

Early adoption signals governance maturity to clients and regulators.

- [ ] Implement basic incident monitoring even for minimal-risk systems.

Good practice — supports post-market vigilance posture.

HIGH-RISK — AI Governance Foundation — ISO 42001 Alignment

- [ ] Establish an AI governance policy approved at board / senior leadership level.

ISO 42001 Clause 5.2 — policy must define objectives, scope, and accountability.

- [ ] Define roles: AI Risk Owner, Data Protection Officer linkage, Technical Accountable Person.
- [ ] Implement an AI inventory — catalogue every AI system with tier, purpose, data inputs.

Foundation for both EU AI Act registration and ISO 42001 Annex A controls.

- [ ] Conduct impact assessments (DPIA where personal data is involved).

Link GDPR Art. 35 DPIA to EU AI Act fundamental rights impact assessment.

- [ ] Establish incident response procedure specific to AI failures and misuse.
- [ ] Schedule annual AI governance review and update cycle.