August 2026 Compliance Deadline

EU AI Act Compliance Checklist 2026

Step-by-Step Implementation Guide — All Four Phases

Primary Keyword: EU AI Act compliance checklist · Covers: Providers, Deployers, GPAI Model Providers

Last updated: March 2026
Source regulation: Regulation (EU) 2024/1689
Website: euaiactguide.com
Author: Martina Fowler, Senior AI Regulatory Counsel

47	4	Aug 2026	€35M
Checklist items	Implementation phases	Primary deadline	Max fine (7% turnover)

Contents

■ **Time check:** As of March 2026, you have approximately 5 months until the August 2026 deadline. Conformity assessments for complex high-risk AI systems take 4–12 months. Start Phase 1 this week.

■ August 2026 — Priority Fast-Track Items

These four items have the longest lead times. Start them immediately regardless of where you are in the four-phase process.

① **Appoint an Authorised Representative [PRIORITY] [Art. 22]**

Identify an EU-established legal entity, execute a written mandate, and register their details. Allow 4–8 weeks. Mandatory for all non-EU providers.

② **Establish Human-in-the-Loop (HITL) Controls [PRIORITY] [Art. 14]**

Build real-time monitoring dashboards, override functions, and halt capabilities into each high-risk AI system. Document oversight procedures.

③ **Compile Annex IV Technical Documentation [PRIORITY] [Art. 11 + Annex IV]**

Assign a documentation lead and systematically complete all Annex IV elements: architecture, training data, testing, accuracy, human oversight, PMM plan.

④ **Register in the EU AI Database [PRIORITY] [Art. 49]**

Complete after conformity assessment. Submit via EU AI Office portal before market placement. Required for all Annex III high-risk systems.

PHASE 1 OF 4

Scoping & Classification

Determine your role, build your AI inventory, and classify every system. This phase sets the scope of all subsequent work.

STEP 1A — IDENTIFY YOUR LEGAL ROLE

- ■ **Determine whether your organisation is a Provider, Deployer, Importer, or Distributor [Art. 3]**
  → *Map every AI system to one of the four actor definitions in Article 3. Document the conclusion for each system in a central AI Registry spreadsheet.*
- ■ **Assess whether modification of third-party AI reclassifies you as a Provider [Art. 25]**
  → *Review each AI tool you have customised or fine-tuned. If modification changes intended purpose or scope, full provider obligations apply.*
- ■ **If non-EU provider: appoint an EU-based Authorised Representative [Art. 22] [PRIORITY]**
  → *Identify a legal entity in the EU, execute a written mandate, register their details with your national competent authority before market placement.*

- [ ] **Build a complete AI System Inventory**

  → *Create a structured register (spreadsheet or GRC tool) capturing: system name, vendor, intended purpose, deployment context, data inputs, and outputs.*

STEP 1B — RISK CLASSIFICATION

- [ ] **Screen all AI systems against the eight Prohibited AI Practices [Art. 5] [PRIORITY]**

  → *Document a written determination for each system. Any positive finding requires immediate shutdown — these bans have been in force since 2 February 2025.*

- [ ] **Screen each AI system against all eight Annex III high-risk categories [Art. 6 + Annex III]**

  → *Cross-reference intended purpose against Annex III: biometrics, critical infrastructure, education, HR, essential services, law enforcement, migration, justice.*

- [ ] **Identify AI safety components embedded in Annex I regulated products [Art. 6(1) + Annex I]**

  → *For each regulated product (medical device, machinery, aviation), assess whether any embedded AI makes safety decisions. If yes, it is high-risk under Annex I.*

- [ ] **Classify remaining systems as Limited Risk (Art. 50 duties) or Minimal Risk [Art. 50]**

  → *Systems interacting with humans (chatbots) or generating synthetic media trigger Art. 50 transparency duties. Document the required disclosure measure for each.*

- [ ] **Document all risk classification decisions with supporting rationale**

  → *Prepare a one-page classification memo per system signed by a senior responsible person. This provides an audit trail if challenged by a surveillance authority.*

- [ ] **Implement AI literacy training for all staff working with AI systems [Art. 4]**

  → *Design role-based training: technical staff need model behaviour awareness; business users need output interpretation; legal teams need regulatory obligation training.*

PHASE 2 OF 4

Gap Analysis

Compare current AI governance practices against Act requirements. Surface exactly what needs to be built, upgraded, or documented.

STEP 2A — GOVERNANCE & POLICY GAPS

- [ ] **Assess your AI governance policy against Article 9 risk management requirements [Art. 9]**
  → *Map existing AI policy against Art. 9 requirements. Record each gap — no lifecycle RMS, no documentation retention, no post-market monitoring — with an owner and deadline.*

- [ ] **Review data governance policies against Article 10 training data requirements [Art. 10]**
  → *Establish a Data Governance Policy including explicit protocols for bias detection, training data diversity, data relevance, and quality thresholds.*

- [ ] **Assess technical documentation practices against Annex IV requirements [Art. 11 + Annex IV]**
  → *For each high-risk system, identify which Annex IV elements exist and which are missing. This gap list becomes Phase 3's technical work plan.*

- [ ] **Evaluate human oversight mechanisms against Article 14 standards [Art. 14]**
  → *Test whether designated humans can in practice: monitor outputs, understand AI reasoning, disregard a recommendation, and stop the system immediately. Document all gaps.*

- [ ] **Audit logging and record-keeping capabilities against Article 12 [Art. 12]**
  → *Verify systems can produce decision-level logs. If not, this is a critical gap requiring engineering work in Phase 3.*

STEP 2B — SUPPLY CHAIN & VENDOR GAPS

- [ ] **Obtain technical documentation from all third-party high-risk AI vendors**
  → *Request conformity assessment summary, Annex IV documentation, and Declaration of Conformity from each AI vendor. Non-provision by mid-2026 is a compliance risk.*

- [ ] **Review AI procurement contracts for EU AI Act compliance warranties**
  → *Add compliance clauses to all AI vendor contracts: require conformity assessment completion, ongoing documentation, incident notification within 15 days, and liability indemnification.*

- [ ] **Assess whether third-party AI is used outside the provider's documented intended purpose [Art. 25]**
  → *Compare each vendor's documented intended purpose against your actual deployment. Out-of-scope use may trigger Article 25 reclassification as Provider.*

STEP 2C — FUNDAMENTAL RIGHTS GAP ASSESSMENT

- [ ] **Conduct Fundamental Rights Impact Assessments (FRIAs) for regulated-sector deployments [Art. 27]**

  → Complete a FRIA for each high-risk AI deployed in public service, employment, credit, or essential services covering: scope, affected populations, rights impacts, and mitigations.

- [ ] **Align existing GDPR DPIAs with FRIA requirements for AI systems processing personal data**

  → Extend existing DPIAs with FRIA-specific questions about fundamental rights impacts beyond privacy to avoid running two entirely separate assessments.

- [ ] **Prioritise gaps into a compliance roadmap with owners, budgets, and August 2026 milestones**

  → Assign each gap a RAG status, a responsible owner, a budget estimate, and a completion date. Target internal completion by April 2026 for high-risk systems.

PHASE 3 OF 4

Technical Implementation

Build or upgrade the technical systems, documentation, and processes required by the Act. Most resource-intensive phase — begin as early as possible.

STEP 3A — RISK MANAGEMENT SYSTEM (ART. 9)

- [ ] **Establish a documented Risk Management System (RMS) for each high-risk AI system [Art. 9]**
  → *Create an RMS document identifying foreseeable risks in normal and misuse conditions, estimating likelihood and severity, and defining mitigation measures. Update after significant changes.*

- [ ] **Define and document residual risk thresholds before deployment [Art. 9(4)]**
  → *Set explicit residual risk acceptance criteria (e.g. false positive rate below X%). Document rationale, approver, and review schedule. Systems exceeding thresholds must not be placed on market.*

STEP 3B — DATA GOVERNANCE (ART. 10)

- [ ] **Implement bias detection and testing protocols for all training datasets [Art. 10(2)(f)]**
  → *Run demographic parity, equal opportunity, and disparate impact tests across all protected characteristics. Document results, corrective actions, and residual bias levels. Repeat after each model update.*

- [ ] **Document training data provenance, quality criteria, and governance procedures [Art. 10(3)]**
  → *For each dataset: document source, date range, coverage, limitations, preprocessing steps, and storage/access controls. This becomes part of Annex IV documentation.*

- [ ] **Where special category data is used in training: document strict necessity justification [Art. 10(5)]**
  → *Use of sensitive data in training is only permitted to detect/correct bias. Document the necessity case, GDPR legal basis, and additional safeguards (minimisation, access restriction, deletion schedule).*

STEP 3C — TECHNICAL DOCUMENTATION (ART. 11 + ANNEX IV)

- [ ] **Compile the Annex IV "Living Document" technical documentation package [Art. 11 + Annex IV] [PRIORITY]**
  → *Assign a documentation lead. Complete all Annex IV elements: architecture, training methodology, dataset descriptions, validation procedures, accuracy metrics, human oversight, and PMM plan.*

- [ ] **Establish documentation version control — Annex IV docs must be kept current**
  → *Store all technical documentation in version-controlled systems with change logs. Any change to training data, architecture, or intended purpose triggers a review within 30 days.*

STEP 3D — LOGGING AND RECORD-KEEPING (ART. 12)

- [ ] **Implement automatic event logging capturing inputs, outputs, and decision parameters [Art. 12]**
  → *Logs must enable post-hoc reconstruction of decisions. Ensure logs are tamper-proof, time-stamped, and accessible to national market surveillance authorities on request.*

- [ ] **Set log retention: deployers retain minimum 6 months; align with sector-specific requirements [Art. 12(1) + Art. 26(5)]**

  → *Build 6-month minimum retention into log storage infrastructure. Cross-reference with DORA, MiFID II, MDR where applicable — sector rules may require longer retention.*

STEP 3E — HUMAN OVERSIGHT (ART. 14)

- [ ] **Design and implement Human-in-the-Loop (HITL) controls [Art. 14] [PRIORITY]**

  → *Build real-time monitoring dashboards, a clearly labelled Override function, and a system halt capability for each high-risk AI system. Train designated oversight personnel.*

- [ ] **Designate named AI Oversight Officers and document their responsibilities [Art. 14(1)]**

  → *Assign a named Oversight Officer per high-risk deployment. Mandate: critically read AI outputs, escalate anomalies, exercise override authority, complete monthly oversight logs.*

- [ ] **Ensure AI systems communicate confidence levels and escalate low-confidence decisions to human review [Art. 14(4)(b)]**

  → *Programme systems to surface confidence scores alongside outputs. Define a threshold below which the system escalates to a human reviewer rather than proceeding autonomously.*

STEP 3F — ACCURACY, ROBUSTNESS AND CYBERSECURITY (ART. 15)

- [ ] **Define accuracy benchmarks and test against independent validation datasets [Art. 15(1)]**

  → *Specify metrics (F1, AUC-ROC, precision/recall) and document target vs achieved accuracy levels. Re-test after each significant model change.*

- [ ] **Implement cybersecurity protections against adversarial attacks, data poisoning, model theft [Art. 15(5)]**

  → *Apply adversarial robustness testing and input validation. Restrict model access. Align with NIST AI RMF cybersecurity controls and document all measures in your Annex IV documentation.*

STEP 3G — INSTRUCTIONS FOR USE AND ARTICLE 50 TRANSPARENCY

- [ ] **Prepare Instructions for Use for each high-risk AI system [Art. 13]**

  → *Draft a document covering: capabilities and limitations, intended/prohibited uses, required oversight measures, logging/maintenance requirements, and technical interface specifications.*

- [ ] **Implement Article 50 transparency disclosures for chatbots, deepfakes, and emotion recognition [Art. 50]**

  → *Chatbots: visible AI disclosure in first interaction. Synthetic media: machine-readable watermarking (e.g. C2PA metadata). AI-generated editorial content: human-readable disclosure label.*

STEP 3H — QUALITY MANAGEMENT SYSTEM (ART. 17)

- [ ] **Establish a Quality Management System covering AI design, development, testing, and monitoring [Art. 17]**

  → *Document your AI compliance strategy, design/development procedures, testing protocols, incident management, and corrective action procedures. Extend an existing ISO 9001 QMS if available.*

- [ ] **Define a post-market monitoring plan specifying production performance tracking [Art. 72]**

  → PMM plan must cover: KPIs to track, data collection method, review frequency, incident escalation thresholds, and corrective action trigger process. Include in Annex IV documentation.

PHASE 4 OF 4

Registration & Filing

Complete formal compliance filings — conformity assessment, Declaration of Conformity, CE marking, and EU AI database registration. These gate your legal right to place the system on the EU market.

STEP 4A — CONFORMITY ASSESSMENT (ART. 43)

- [ ] **Conduct conformity assessment verifying compliance with Articles 8–15 [Art. 43]**
  → *Most Annex III systems use internal self-assessment. Work through each Art. 8–15 requirement and record compliance evidence. Appoint a senior reviewer to sign off the assessment.*

- [ ] **For biometric ID systems and Annex I products: engage an accredited Notified Body [Art. 43(1)]**
  → *Identify a Notified Body via the EU NANDO database. Engage at least 6 months before target market placement — Notified Bodies have significant lead times and limited capacity.*

STEP 4B — DECLARATION OF CONFORMITY AND CE MARKING

- [ ] **Prepare and sign the EU Declaration of Conformity for each high-risk AI system [Art. 47]**
  → *DoC must contain: provider identity, system description, conformity statement, standards applied, date and place, and authorised signatory. Use Annex V as template.*

- [ ] **Affix CE marking to high-risk AI system products [Art. 48]**
  → *CE marking must be visible and legible on the system (or packaging/documentation for non-physical AI). If embedded in an Annex I product, the product CE marking covers the AI component.*

STEP 4C — EU AI DATABASE REGISTRATION

- [ ] **Register each high-risk Annex III AI system in the EU AI database before market placement [Art. 49] [PRIORITY]**
  → *Submit via EU AI Office portal: provider identity, system description, intended purpose, geographic scope, conformity assessment summary, and DoC reference. Retain registration number.*

- [ ] **If deployer of high-risk AI in public-service contexts: register your deployment [Art. 49(2)]**
  → *Deployers in law enforcement, migration, justice, and education must register their specific deployment separately from the provider's registration. Check national authority procedure.*

STEP 4D — POST-MARKET OBLIGATIONS

- [ ] **Activate post-market monitoring from day of deployment [Art. 72]**
  → *Implement your PMM plan. Set up automated dashboards tracking defined KPIs. Schedule quarterly AI governance reviews. Report material deviations from benchmarks to senior leadership.*

- [ ] **Establish a serious incident reporting procedure — 15-day notification required [Art. 73]**
  → *Define serious incident criteria aligned with Art. 3(49). Train operations staff to escalate immediately. The 15-day clock starts from first awareness — internal delays count against this window.*

- [ ] **Retain all compliance records for 10 years from market placement [Art. 18]**

  → *Set a document retention lock in your DMS for all technical documentation, conformity assessments, and DoCs. National authorities can request these documents at any time during retention.*

ROLE-SPECIFIC

Deployer-Specific Obligations

These items apply specifically to organisations using (but not building) high-risk AI systems, in addition to the Phase 1–4 items above.

- [ ] **Verify each high-risk AI you deploy has a completed conformity assessment and valid DoC from the provider [Art. 26(1)]**

  → *Request the DoC and conformity assessment summary from every vendor. Non-provision is a red flag creating direct regulatory exposure.*

- [ ] **Use each high-risk AI only within the scope and conditions in the provider's Instructions for Use [Art. 26(1)]**

  → *Maintain a copy of each vendor's Instructions for Use and circulate relevant sections to operational teams. Require manager sign-off for any novel deployment context.*

- [ ] **Implement human oversight measures specified by the provider and train oversight personnel [Art. 26(2)]**

  → *Take oversight requirements from the Instructions for Use and translate into internal procedures. Run tabletop exercises simulating AI anomalies to verify your override procedures work.*

- [ ] **Maintain use logs for each high-risk AI system for minimum 6 months [Art. 26(5)]**

  → *Configure systems to generate and retain Article 12 compliant logs. Build log review into your quarterly AI governance cycle.*

- [ ] **Implement right-to-explanation and complaint procedures for AI-assisted individual decisions [Art. 26(10)]**

  → *Establish a documented procedure for individuals to request explanation of AI-influenced decisions (credit denial, job rejection). Align with GDPR Article 22 procedure if one exists.*

ROLE-SPECIFIC

GPAI Model Provider Obligations

These items apply to developers of General Purpose AI models (foundation models, LLMs). Obligations applied from 2 August 2025.

- [ ] **Prepare and maintain technical documentation of GPAI model training methodology, capabilities, and limitations [Art. 53(1)(a)]**

  → *Document training data sources/volumes, compute (FLOPs), architecture, benchmarks, limitations, and safety testing results. Must be available to EU AI Office on request.*

- [ ] **Publish a training data content summary sufficient for downstream providers to assess the model [Art. 53(1)(d)]**

  → *Publish a model card covering: data categories, geographic representation, cutoff dates, and significant exclusions. Category-level summary is sufficient; proprietary details not required.*

- [ ] **Implement and document a copyright compliance policy for training data [Art. 53(1)(c)]**

  → Establish a data sourcing policy requiring copyright review before any web-scraped dataset is used in training. Document rights clearances and opt-out mechanism compliance.

- [ ] **If model exceeds systemic risk threshold (10^25 FLOPs): notify EU AI Office and complete adversarial testing [Art. 51-55]**

  → Submit notification to EU AI Office. Commission red-team testing covering harmful content, CBRN risk uplift, and cybersecurity capabilities. Report serious incidents within 15 days.

Authoritative Sources

- EUR-Lex Official Text: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
- EU AI Office: digital-strategy.ec.europa.eu/en/policies/ai-office
- NIST AI Risk Management Framework: nist.gov/artificial-intelligence
- ISO 42001 AI Management System: iso.org/standard/81230.html
- CEN-CENELEC AI Harmonised Standards: cencenelec.eu
- OECD AI Principles: oecd.ai/en/ai-principles
- IAPP EU AI Act Resource Centre: iapp.org/resources/article/eu-ai-act-resource-center
- EDPB GDPR & AI Guidance: edpb.europa.eu