EU AI Act
Compliance Checklist

The Complete Guide to EU AI Act Requirements

2025 Edition

This comprehensive checklist helps you understand and track your EU AI Act compliance obligations. Use it to assess your AI systems, identify requirements, and monitor your compliance progress.

■ Quick Facts

- **Penalties:** Up to €35M or 7% of global revenue
- **Timeline:** High-risk compliance by August 2026
- **Scope:** Any AI system affecting EU users
- **Articles:** 113 requirements for high-risk AI

Table of Contents

1. Understanding the EU AI Act

The EU AI Act is the world's first comprehensive law regulating artificial intelligence. It establishes a risk-based framework that categorizes AI systems by their potential impact on safety and fundamental rights.

Risk Levels

Risk Level	Description	Requirements
■ Prohibited	Banned AI practices (social scoring, real-time biometric ID in public)	Cannot be deployed in EU
■■ High-Risk	AI in critical areas (hiring, healthcare, education, law enforcement)	Full compliance: Articles 9-15, conformity assessment
■ Limited Risk	Chatbots, emotion recognition, deepfakes	Transparency requirements only
■ Minimal Risk	Most AI applications (spam filters, games, etc.)	No specific requirements

Key Deadlines

Date	Milestone	Status
Feb 2, 2025	Prohibited AI practices banned	■ ACTIVE
Aug 2, 2025	GPAI transparency rules apply	■ ACTIVE
Aug 2, 2026	High-risk AI systems must comply	■ 8 months
Aug 2, 2027	Legacy high-risk systems in regulated products	■ 20 months

■ Who Must Comply?

Any organization that develops, deploys, imports, or distributes AI systems that affect EU users—regardless of where the organization is located. This includes US companies serving European customers.

2. Risk Classification Checklist

Use this checklist to determine your AI system's risk classification.

■ Prohibited AI Practices (Article 5)

Check if your AI system does any of the following:

- ■ Social scoring by public authorities
- ■ Exploitation of vulnerabilities (age, disability, economic situation)
- ■ Real-time remote biometric identification in public spaces
- ■ Emotion recognition in workplace or education (with exceptions)
- ■ Biometric categorization inferring sensitive characteristics
- ■ Untargeted scraping of facial images for facial recognition databases
- ■ Predictive policing based solely on profiling

■■ If any box is checked

Your AI system may be prohibited under the EU AI Act and cannot be deployed in the EU. Consult legal counsel immediately.

■■ High-Risk AI Systems (Annex III)

Check if your AI is used in any of these areas:

- ■ Biometric identification and categorization
- ■ Critical infrastructure management (water, gas, electricity, traffic)
- ■ Education and vocational training (admissions, assessments, cheating detection)
- ■ Employment (recruitment, hiring, task allocation, performance evaluation, termination)
- ■ Access to essential services (credit scoring, emergency services, health/life insurance)
- ■ Law enforcement (risk assessment, evidence evaluation, crime prediction)
- ■ Migration and border control (document verification, visa applications)
- ■ Administration of justice (legal research, case outcome prediction)
- ■ Democratic processes (election influence, political behavior)

■ If any box is checked

Your AI system is likely HIGH-RISK and must comply with Articles 9-15. Continue to Section 3 for detailed requirements.

3. High-Risk AI Requirements

High-risk AI systems must comply with Articles 9-15 of the EU AI Act. Use this section to track your compliance with each requirement.

Article 9: Risk Management System

Establish and maintain a risk management system throughout the AI system lifecycle:

■ Identification and analysis of known and foreseeable risks

■ Estimation and evaluation of risks from intended use and misuse

■ Risk mitigation measures implemented and documented

■ Residual risks communicated to deployers

■ Testing procedures to identify appropriate risk management measures

■ Risk management process documented and updated regularly

■ Consideration of risks to health, safety, and fundamental rights

Article 10: Data and Data Governance

Ensure training, validation, and testing data meets quality standards:

■ Data governance and management practices documented

■ Training data relevant, representative, and free from errors

■ Appropriate statistical properties for intended use verified

■ Potential biases identified and addressed

■ Data gaps and shortcomings documented

■ Personal data processing compliant with GDPR

■ Bias detection and correction measures in place

Article 11: Technical Documentation

Prepare comprehensive technical documentation including:

■ General description of the AI system

■ Detailed description of system elements and development process

■ Information about monitoring, functioning, and control

■ Description of the risk management system

■ Description of changes made throughout lifecycle

■ List of harmonised standards applied

■ EU declaration of conformity prepared

■ Detailed description of system performance and limitations

Article 12: Record-Keeping

Implement automatic logging capabilities:

■ Automatic logging of events enabled throughout operation

■ Logs include period of use for each application

■ Reference database usage logged (if applicable)

■ Input data logged or can be reconstructed

■ Logs enable traceability of AI system functioning

■ Logs stored for appropriate duration (lifetime of system)

■ Log integrity protected (tamper-evident)

■ Logs accessible for auditing purposes

Article 13: Transparency and Information

Ensure transparency to deployers and users:

■ Instructions for use provided to deployers

■ AI system capabilities and limitations documented

■ Intended purpose clearly specified

■ Level of accuracy and performance metrics disclosed

■ Known circumstances that may impact performance documented

■ Human oversight measures specified

■ Expected lifetime and maintenance requirements documented

Article 14: Human Oversight

Enable effective human oversight of the AI system:

■ Human oversight measures designed into the system

■ Humans can understand AI system capabilities and limitations

■ Humans can monitor operation and detect anomalies

■ Humans can interpret AI system output correctly

■ Humans can decide not to use the system or override output

■ Humans can intervene or interrupt operation

■ Stop button or similar procedure available for high-risk cases

■ Oversight measures documented and communicated

Article 15: Accuracy, Robustness, and Cybersecurity

Ensure appropriate levels of accuracy and security:

■ Accuracy levels appropriate for intended purpose

■ Accuracy levels declared in instructions for use

■ Resilient against errors, faults, and inconsistencies

■ Redundancy measures (backup, fail-safe) implemented where appropriate

■ Robust against attempts by unauthorized parties to manipulate

■ Protected against adversarial attacks and data poisoning

■ Cybersecurity measures appropriate to risks

■ Technical solutions address AI-specific vulnerabilities

■ Compliance Score

Count your checked boxes above. For full compliance with high-risk requirements, you should have 55+ items completed. Any unchecked items represent compliance gaps that need to be addressed before the August 2026 deadline.

4. GPAI Model Requirements

General Purpose AI (GPAI) models, including foundation models like GPT-4 and Claude, have specific transparency obligations under the EU AI Act.

All GPAI Providers

If you provide a GPAI model:

- ■ Technical documentation prepared and maintained
- ■ Information provided to downstream AI system providers
- ■ Policy for respecting EU copyright law established
- ■ Detailed summary of training content published

GPAI with Systemic Risk

If your GPAI model has systemic risk (>10^25 FLOPs training):

- ■ Model evaluation performed according to standardized protocols
- ■ Systemic risks assessed and mitigated
- ■ Serious incidents tracked and reported to AI Office
- ■ Adequate cybersecurity protection ensured
- ■ Energy consumption and environmental impact documented

5. Transparency Requirements

Limited risk AI systems have specific transparency obligations.

Chatbots & Conversational AI

- ■ Users informed they are interacting with an AI system
- ■ Disclosure provided before or at start of interaction
- ■ Disclosure is clear and understandable

Emotion Recognition & Biometric Categorization

- ■ Individuals informed of system operation
- ■ Purpose of system disclosed
- ■ Personal data processed in accordance with GDPR

AI-Generated Content (Deepfakes)

- ■ Content labeled as artificially generated or manipulated
- ■ Labeling is machine-readable where technically feasible
- ■ Exception: Artistic, satirical, or editorial content (with disclosure)

6. Documentation Checklist

Use this checklist to track required compliance documentation.

Required Documents

■ **Technical Documentation** — Comprehensive system description per Annex IV

■ **Risk Management System** — Risk assessment, mitigation measures, monitoring

■ **Data Governance Policy** — Data quality, bias assessment, GDPR compliance

■ **Human Oversight Procedures** — How humans monitor and intervene

■ **Instructions for Use** — Information for deployers and users

■ **Quality Management System** — Procedures ensuring ongoing compliance

■ **EU Declaration of Conformity** — Self-declaration of compliance

■ **Incident Reporting Procedures** — How to report serious incidents

Supporting Evidence

■ **Model Cards** — Documentation of ML model characteristics

■ **Training Data Documentation** — Data sources, processing, quality measures

■ **Testing & Validation Reports** — Performance metrics, bias testing results

■ **Security Assessment** — Cybersecurity measures, penetration tests

■ **Audit Trail Samples** — Evidence of logging capabilities

■ **Change Log** — Record of system modifications

7. Compliance Timeline

Plan your compliance journey with these key milestones.

Immediate Actions (Now)

- ■ Inventory all AI systems in your organization
- ■ Classify each system by risk level
- ■ Identify high-risk systems requiring full compliance
- ■ Assign compliance ownership and budget

Q1-Q2 2026

- ■ Complete risk assessments for all high-risk systems
- ■ Begin technical documentation
- ■ Implement logging and audit trail capabilities
- ■ Establish human oversight procedures

Q3 2026 (Before August Deadline)

- ■ Finalize all required documentation
- ■ Complete conformity assessment
- ■ Register in EU database (if required)
- ■ Prepare EU Declaration of Conformity
- ■ Brief stakeholders on compliance status

Ongoing

- ■ Monitor AI system performance
- ■ Update documentation as system changes
- ■ Report serious incidents
- ■ Conduct regular compliance reviews

8. Getting Started with Protectron

Protectron helps you achieve EU AI Act compliance faster and more efficiently than traditional approaches. Here's how to get started:

What Protectron Provides

✓ **Risk Classification**: Instantly classify your AI systems and understand your obligations

✓ **Requirement Tracking**: Track all 113 high-risk requirements with real-time progress

✓ **Document Generation**: AI-powered generation of technical documentation and policies

✓ **Agent Audit Trail**: Automatic logging for LangChain, CrewAI, and custom AI agents

✓ **Evidence Management**: Organize and link evidence to requirements

✓ **Certification Badges**: Verifiable compliance badges for your website

■ **Start Your Free Trial**

protectron.ai

- Free risk assessment in 10 minutes
- No credit card required
- Start tracking compliance immediately

Questions? Contact us at **hello@protectron.ai**

Ready to get compliant?

Visit **protectron.ai** to start your free trial today.

Stop risking €35 million fines. Start building compliant AI.