

EU AI ACT COMPLIANCE CHECKLIST

AI SYSTEM CLASSIFICATION & REGULATORY OBLIGATIONS

NABIHA HERRADI
AI GOVERNANCE, RISK & COMPLIANCE ADVISOR

Purpose

This checklist is designed to support the classification of AI systems and the identification of applicable obligations under the EU AI Act. It enables organizations to assess risk levels, document governance controls, and establish a foundation for regulatory compliance and audit readiness.

SECTION 1 — AI SYSTEM OVERVIEW

Field	Details
AI System Name	
Business Function / Use Case	
System Owner	
Deployment Type (Internal / External / Third-Party)	
Data Types Processed (PII, Sensitive, etc.)	
Geographic Scope (EU / Global)	

SECTION 2 — Risk Classification (EU AI ACT)

Requirement	Status (/)	Notes
AI system classification performed		
System evaluated against prohibited AI criteria		
System assessed for high-risk classification		
Use case involves employment, biometric identification, or critical services		
Risk level documented (Prohibited / High-Risk / Limited / Minimal)		

SECTION 3 – High-Risk Requirements (If Applicable)

Requirement	Status	Notes
Risk management system implemented and maintained		
Data governance and data quality controls defined		
Technical documentation prepared and maintained		
Human oversight mechanisms established		
Accuracy, robustness, and cybersecurity measures implemented		
Logging and traceability capabilities enabled		

SECTION 4 - Transparency & Disclosures

Requirement	Status	Notes
Users are informed that AI is in use		
AI-generated content is clearly labeled		
Instructions for use and limitations are documented		
Transparency requirements assessed for applicable use case		

SECTION 5- Governance & Accountability

Requirement	Status	Notes
Responsible AI owner formally assigned		
Roles and responsibilities clearly defined		
AI governance policies and procedures documented		

Requirement	Status	Notes
Review and approval process established		
Compliance documentation stored and maintained		

SECTION 6 - Third-party & Vendor Risk

Requirement	Status	Notes
Third-party AI systems identified		
Vendor risk assessment completed		
Contracts include AI compliance and data protection clauses		
Vendor responsibilities clearly defined		

SECTION 7- Monitoring & Continuous Compliance

Requirement	Status	Notes
Ongoing monitoring process established		
Periodic risk reassessment performed		
Model performance and drift monitored		
Incident management and escalation defined		

SECTION 8- Gap Analysis & Action Plan

Area	Gap Identified	Recommended Action	Owner	Timeline



Prepared by Sofia Nabiha Herradi <u>AI Governance & Compliance Advisory</u>	info@aigrcadvisory.com aigrcadvisory.com linkedin.com/in/sofia-Nabiha-Herradi
--	--