Forge.io

SOVEREIGN HEALTHCARE CLOUD

AI-ACT COMPLIANCE BRIEF

EU AI Act: Model Hosting Implications

Proactive compliance framework for high-risk AI system deployment

Sheraz Bhatti, Global CTO - Forge.io

Nov 28, 2025

Executive Summary

The EU Artificial Intelligence Act (Regulation 2024/1689) establishes a comprehensive regulatory framework for AI systems operating within the European Union. For organisations deploying high-risk AI systems-particularly in healthcare, critical infrastructure, and biometric identification-compliance requires demonstrable technical controls that go beyond policy assertion.

Forge infrastructure provides architectural enforcement of AI Act requirements, reducing compliance burden from procedural documentation to verifiable system properties.

High-Risk Classification

Under Article 6 and Annex III, AI systems used in healthcare contexts are classified as high-risk. This includes diagnostic assistance systems, treatment recommendation engines, medical imaging analysis, and any AI that influences clinical decision-making.

Annex III High-Risk Categories (Healthcare Relevant): 5(a) - AI intended to be used as safety components in medical devices 5(b) - AI systems that are themselves medical devices or IVD medical devices 6(a) - Remote biometric identification systems 6(b) - AI for determining access to healthcare services or emergency response

Article-by-Article Compliance

Art. 9 - Risk Management System IsoCell isolation enables per-model risk containment. Forge Observe provides continuous monitoring with automated anomaly detection.

Art. 10 - Data and Data Governance Jurisdiction-locked storage ensures training data never leaves designated regions. Hardware-enforced isolation prevents data contamination between models.

Art. 11 - Technical Documentation Automated documentation generation from infrastructure telemetry. Model cards populated from runtime observations.

Art. 12 - Record-Keeping LGTM stack provides comprehensive observability. Loki captures all logs with tamper-evident storage. Tempo traces every inference request.

Transparency and Oversight

Art. 13 - Transparency and Provision of Information Model behavior dashboards expose decision patterns. Inference tracing shows reasoning paths. Confidence scores and uncertainty measures are surfaced through Grafana visualisations.

Art. 14 - Human Oversight Administrative control plane operates outside model execution context. Immediate intervention capability via kill switches. Automated alerts on anomalous behavior with human-in-the-loop escalation.

Art. 15 - Accuracy, Robustness, and Cybersecurity Hardware-isolated execution via MicroVMs. Zero ambient access architecture. Ephemeral compute prevents persistent compromise. Network isolation via ForgeMesh eliminates lateral movement vectors.

Compliance Properties

Risk Management: Continuous, automated Data Governance: Jurisdiction-locked Documentation: Auto-generated from telemetry Record Keeping: LGTM stack, immutable Transparency: Full observability Human Oversight: Control plane + kill switches

Conclusion

The AI Act distinguishes between providers (who develop AI systems) and deployers (who use them). Healthcare organisations deploying AI models on Forge infrastructure benefit from a simplified compliance posture: provider obligations are met through infrastructure controls, while deployer requirements are enabled through built-in observability and oversight mechanisms.

Compliance is not a document. It is an architectural property.