Unimedia •Tech

AI Act Compliance Checklist for CTOs

Practical governance, audit, and security guide
to comply with the
European Union’s AI regulation.

1. Risk Classification and Assessment

- ▫ Does the system use generative, predictive, or decision-making AI?
- ▫ Have you classified each system under the AI Act (minimal, limited, high-risk)?
- ▫ Do you maintain an inventory of models, datasets, and external APIs used?

2. Technical Documentation and Traceability

- ▫ Do you have up-to-date technical documentation of the model and its architecture?
- ▫ Do you use a model versioning system (model registry)?
- ▫ Do you log automated decisions and outputs for auditability?

3. Human Oversight

- ▫ Is there a clear human intervention process for critical decisions?
- ▫ Are defined roles responsible for supervising, reviewing, and approving the model?
- ▫ Are users informed when interacting with an AI system?

4. Data, Security, and Privacy

- ▫ Do the datasets comply with GDPR and other relevant regulations?
- ▫ Do you have controls to detect and mitigate bias or unintended impacts?
- ▫ Is the system protected against adversarial attacks and information leaks?

5. Model Lifecycle Management

- ▫ Is the model's performance continuously monitored in production?
- ▫ Do you retrain the model when data or business context changes?
- ▫ Do you have processes to correct, disable, or retire models if risks arise?

6. Cloud Infrastructure and Auditability

- ▫ Does your cloud architecture meet security and traceability requirements?
- ▫ Do you control resource usage to avoid insecure configurations or unexpected costs?
- ▫ Do you use EU-aligned tools, such as Cloud-Trim, to optimize and audit AWS environments?

7. Audit Readiness

- ▫ Do you have all required documentation for an AI Act compliance audit?
- ▫ Can you provide evidence of human oversight, risk mitigation, and model traceability?
- ▫ Is there a designated person or team responsible for AI Act compliance?