EU AI Act Compliance Checklist

A Practical Guide for US Companies

Published by DigiForm Solutions
Your Partner in AI Governance & Digital Transformation

Introduction

The EU Artificial Intelligence Act represents the world's first comprehensive AI regulation, with enforcement beginning August 2, 2027. This checklist provides US companies with a practical framework for achieving compliance, avoiding penalties up to €35M or 7% of global turnover, and maintaining market access in the European Union.

Who This Guide Is For:

- US companies with AI systems accessible to EU users
- Software providers selling to European customers
- Organizations with APIs or services available from EU IP addresses
- Compliance officers, legal counsel, and technical teams responsible for AI governance

---

Phase 1: Initial Assessment (Weeks 1-4)

System Inventory & Classification

☐ Create Complete AI System Inventory

- List all AI systems, tools, and models currently deployed

- Include third-party AI services and APIs your organization uses
- Document AI-powered features within larger software products
- Identify systems accessible to EU users (directly or indirectly)

☐ Determine EU AI Act Applicability

- Confirm if your AI outputs reach EU users
- Check if your software is sold to EU customers
- Verify if your APIs are accessible from European IP addresses
- Review contracts with EU-based clients or partners

☐ Classify Each AI System by Risk Level

- **Unacceptable Risk:** Social scoring, real-time biometric surveillance, manipulation systems
- **High Risk:** Employment tools, credit scoring, healthcare diagnostics, education assessment, law enforcement, critical infrastructure
- **Limited Risk:** Chatbots, emotion recognition, deepfake generation
- **Minimal Risk:** Spam filters, recommendation engines, inventory management

☐ Prioritize High-Risk Systems

- Focus compliance efforts on high-risk AI first
- Document why each system falls into its risk category
- Prepare justification for classification decisions

Phase 2: Gap Analysis (Weeks 5-8)

Technical Requirements Assessment

☐ Risk Management System

- ☐ Current risk assessment process documented
- ☐ Continuous monitoring mechanisms in place
- ☐ Post-market surveillance data collection active

- ☐ Foreseeable misuse scenarios identified
- ☐ Risk mitigation measures defined

☐ Data Governance

- ☐ Training data quality standards established
- ☐ Dataset representativeness validated
- ☐ Bias detection and mitigation processes implemented
- ☐ Data provenance and lineage tracked
- ☐ Statistical properties documented

☐ Technical Documentation

- ☐ System design and architecture documented
- ☐ Development methodology described
- ☐ Testing and validation procedures recorded
- ☐ Performance metrics and limitations specified
- ☐ Update and modification history maintained

☐ Record-Keeping & Logging

- ☐ Automatic logging capabilities built
- ☐ Log retention periods defined (minimum 6 months)
- ☐ Audit trail for all system decisions
- ☐ User interaction history captured
- ☐ Log security and integrity ensured

☐ Transparency & Information

- ☐ User instructions and documentation prepared
- ☐ System capabilities and limitations clearly stated
- ☐ Intended purpose and use cases defined
- ☐ Human oversight requirements specified
- ☐ Contact information for support provided

☐ Human Oversight

- ☐ Human-in-the-loop mechanisms designed
- ☐ Override capabilities implemented
- ☐ Stop functionality available
- ☐ Oversight personnel identified and trained
- ☐ Escalation procedures established

☐ Accuracy, Robustness & Cybersecurity

- ☐ Accuracy benchmarks defined and measured
- ☐ Robustness testing against edge cases completed
- ☐ Cybersecurity measures implemented
- ☐ Resilience to attacks validated
- ☐ Error handling and recovery procedures documented

Phase 3: Compliance Implementation (Weeks 9-20)

Building Compliant Systems

☐ Establish Risk Management Framework

- Implement continuous risk assessment process
- Create risk register for each high-risk AI system
- Define risk acceptance criteria and thresholds
- Establish feedback loop from post-market data
- Assign risk management ownership and accountability

☐ Enhance Data Governance

- Audit training datasets for quality and bias
- Implement bias detection and mitigation tools
- Document data sources and collection methods
- Establish data quality monitoring processes
- Create procedures for dataset updates and versioning

☐ **Create Technical Documentation**

- Prepare EU declaration of conformity template
- Document system architecture and design decisions
- Record development and testing methodologies
- Specify performance metrics and evaluation criteria
- Maintain version control and change logs

☐ **Implement Logging & Monitoring**

- Deploy automatic logging infrastructure
- Configure log retention and archival systems
- Establish log analysis and review procedures
- Implement alerting for anomalous behavior
- Ensure log tamper-evidence and security

☐ **Develop User-Facing Materials**

- Write clear instructions for deployers and users
- Create transparency notices for end users
- Prepare capability and limitation disclosures
- Develop training materials for human oversight personnel
- Establish support and contact channels

☐ **Design Human Oversight Mechanisms**

- Implement human-in-the-loop workflows where required
- Build override and stop functionality
- Train oversight personnel on AI system operation
- Establish escalation and incident response procedures
- Document oversight responsibilities and authorities

☐ **Strengthen Security & Robustness**

- Conduct adversarial testing and red-teaming
- Implement cybersecurity controls and monitoring

- Validate system resilience to attacks and failures
- Establish incident response and recovery procedures
- Document security architecture and controls

Phase 4: Conformity Assessment (Weeks 21-28)

Demonstrating Compliance

☐ Determine Conformity Assessment Path

- Check if third-party assessment is required (Annex VII systems)
- Identify appropriate notified body if needed
- Prepare for internal assessment if self-certification allowed
- Understand assessment scope and requirements

☐ Prepare Assessment Documentation

- Compile technical documentation package
- Gather evidence of compliance with each requirement
- Prepare test results and validation reports
- Document risk management process and outcomes
- Collect post-market surveillance data (if available)

☐ Conduct Internal Review

- Perform gap analysis against all AI Act requirements
- Validate completeness of technical documentation
- Review risk management system effectiveness
- Test logging and monitoring capabilities
- Verify human oversight mechanisms

☐ Engage Notified Body (if required)

- Submit documentation to selected notified body

- Respond to information requests and clarifications
- Address any non-conformities identified
- Obtain conformity certificate

☐ **Issue EU Declaration of Conformity**

- Complete declaration template with all required information
- Sign declaration by authorized representative
- Affix CE marking to AI system (if applicable)
- Make declaration available to authorities upon request

Phase 5: Market Placement & Ongoing Compliance (Week 29+)

Maintaining Compliance

☐ **Register in EU Database**

- Register high-risk AI systems in EU database before market placement
- Provide required information (name, intended purpose, risk classification)
- Update registration for significant changes
- Maintain registration accuracy

☐ **Establish Post-Market Monitoring**

- Implement systematic data collection on AI performance
- Monitor for incidents, malfunctions, and unexpected behavior
- Track user feedback and complaints
- Analyze performance against intended purpose
- Feed findings back into risk management system

☐ **Report Serious Incidents**

- Define criteria for serious incidents requiring reporting

- Establish incident reporting procedures and timelines
- Designate responsible personnel for incident management
- Prepare incident report templates
- Maintain incident log and corrective action tracking

☐ **Maintain Documentation**

- Keep technical documentation up to date
- Retain logs for required periods (minimum 6 months)
- Document all system updates and modifications
- Maintain conformity assessment records
- Prepare for potential authority inspections

☐ **Conduct Periodic Reviews**

- Review risk management system effectiveness annually
- Reassess system classification if functionality changes
- Update technical documentation for significant changes
- Refresh conformity assessment if required
- Train personnel on updated procedures

Risk Assessment Matrix

Use this matrix to evaluate and prioritize AI systems for compliance:

Risk Factor	Low (1)	Medium (2)	High (3)	Critical (4)
Impact on Fundamental Rights	Minimal	Moderate	Significant	Severe
Safety Consequences	None	Minor	Major	Life-threatening
EU User Exposure	<100 users	100-10K users	10K-1M users	>1M users
Decision Autonomy	Human decides	Human reviews	AI recommends	AI decides
Reversibility	Easily reversed	Reversible with effort	Difficult to reverse	Irreversible

Risk Score Calculation: Sum scores across all factors

- **5-8:** Likely Minimal Risk
- **9-12:** Likely Limited Risk
- **13-16:** Likely High Risk
- **17-20:** Potentially Unacceptable Risk

Vendor Evaluation Template

When assessing third-party AI systems for EU AI Act compliance:

Vendor Information

- **Vendor Name:** _____
- **AI System Name:** _____
- **Intended Use:** _____
- **Risk Classification:** ☐ Minimal ☐ Limited ☐ High ☐ Unacceptable

Compliance Questions

☐ Has the vendor confirmed EU AI Act compliance?

- Request written confirmation and supporting documentation

☐ **Is technical documentation available?**

- System design, development methodology, performance metrics

☐ **Are conformity assessment records provided?**

- EU declaration of conformity, CE marking (if applicable), notified body certificate

☐ **Does the system provide required logging?**

- Automatic logging, log retention, audit trail capabilities

☐ **Are transparency materials included?**

- Instructions for use, capability disclosures, limitation statements

☐ **Is human oversight supported?**

- Override mechanisms, stop functionality, escalation procedures

☐ **What post-market monitoring does the vendor conduct?**

- Incident tracking, performance monitoring, user feedback collection

☐ **How are updates and modifications handled?**

- Change notification, re-assessment requirements, documentation updates

☐ **What support is provided for compliance?**

- Training, documentation, technical support, compliance assistance

☐ **Are contractual protections in place?**

- Compliance warranties, indemnification, audit rights, termination for non-compliance

---

Common Compliance Pitfalls to Avoid

❌ **Misclassifying AI Systems**

- Underestimating risk level to avoid compliance burden
- Failing to recognize when general-purpose AI becomes high-risk in specific use
- Not reassessing classification when system functionality changes

❌ **Inadequate Documentation**

- Treating documentation as a one-time exercise rather than continuous process
- Failing to document design decisions and trade-offs
- Not maintaining version control and change history

❌ **Insufficient Data Governance**

- Assuming training data is representative without validation
- Failing to detect and mitigate bias systematically
- Not documenting data sources, collection methods, and limitations

❌ **Weak Human Oversight**

- Implementing oversight as a formality rather than meaningful control
- Not training oversight personnel adequately
- Failing to empower humans to override AI decisions

❌ **Delayed Compliance Start**

- Waiting until 2027 to begin compliance efforts
- Underestimating time required for conformity assessment
- Not accounting for third-party dependencies and lead times

❌ **Ignoring Third-Party AI**

- Assuming vendor compliance without verification
- Failing to establish contractual protections
- Not maintaining oversight of vendor-provided AI systems

❌ **Neglecting Post-Market Monitoring**

- Treating compliance as a pre-launch checkbox
- Not collecting performance data systematically

- Failing to act on incidents and user feedback

Next Steps: How DigiForm Can Help

Achieving EU AI Act compliance requires expertise across legal, technical, and operational domains. DigiForm Solutions specializes in helping US companies navigate this complex regulatory landscape.

Our AI Governance Services

Compliance Readiness Assessment

- Comprehensive AI system inventory and classification
- Gap analysis against EU AI Act requirements
- Risk prioritization and compliance roadmap
- Timeline and resource planning

Framework Design & Implementation

- Risk management system design
- Data governance framework development
- Technical documentation templates
- Logging and monitoring architecture

Conformity Assessment Support

- Documentation package preparation
- Internal compliance review
- Notified body engagement coordination
- EU declaration of conformity preparation

Ongoing Compliance Management

- Post-market monitoring program design
- Incident reporting procedures

- Periodic compliance reviews
- Training and enablement

Schedule Your AI Governance Assessment

Don't wait until the August 2027 deadline. Start your compliance journey today with a comprehensive assessment from DigiForm's AI governance experts.

Contact Us:

- **Email:** hello@digiform.io
- **Phone:** +1 305-204-2948
- **Website:** https://digiform.io/ai-governance-advisory

About DigiForm Solutions

DigiForm Solutions is an AI governance and digital transformation consultancy that helps enterprises adopt artificial intelligence responsibly while maintaining compliance and accountability. With 60+ AI projects governed and zero compliance incidents, we've established a proven track record in enterprise AI transformation.

Our expertise spans AI Governance & Advisory, Regulated Industries & Scientific Intelligence, Digital Professional Services, and Media & Intelligence through The Context Window newsletter.

Learn More:

- AI Governance Services: https://digiform.io/ai-governance-advisory
- Blog & Insights: https://digiform.io/blog
- The Context Window Newsletter: Subscribe at https://digiform.io

---

This checklist is provided for informational purposes and does not constitute legal advice. Consult with qualified legal counsel for guidance on your specific compliance obligations.