Hyperion Consulting

Strategic Compliance Guide

EU AI Act

Complete Implementation Framework

The European Union's Artificial Intelligence Act is the world's first comprehensive regulatory framework for AI. Effective August 2024, with key compliance deadlines through 2027, it establishes binding requirements based on risk classification.

This guide provides a strategic roadmap for achieving compliance, with particular focus on high-risk AI systems subject to the most stringent obligations.

Edition	January 2026
Primary Deadline	August 2, 2026
Maximum Penalty	€35M or 7% global turnover
Scope	All AI systems in the EU market

hyperion-consulting.io contact@hyperion-consulting.io

Contents

1 Executive Summary

The EU AI Act (Regulation 2024/1689) entered into force on August 1, 2024, marking the beginning of a phased implementation period. Organizations operating in the EU market must understand their obligations and take action to achieve compliance.

1.1 Strategic Implications

Market Access. Non-compliant AI systems cannot be placed on the EU market or put into service. This affects both EU-based organizations and any entity whose AI systems impact EU citizens.

Financial Exposure. Penalties are substantial: up to €35 million or 7% of worldwide annual turnover for the most serious violations. Even minor infractions can result in fines of €7.5 million or 1% of turnover.

Operational Impact. High-risk AI systems require significant compliance infrastructure including risk management systems, technical documentation, human oversight mechanisms, and post-market monitoring.

Competitive Advantage. Early compliance can differentiate organizations in the market. The EU's approach is likely to influence global AI regulation, making compliance investments valuable beyond the EU.

1.2 Key Dates

Date	Milestone
August 1, 2024	AI Act entered into force
February 2, 2025	Prohibited practices and AI literacy obligations became enforceable
August 2, 2025	Governance and GPAI model obligations took effect
January 2026	**Current date**
August 2, 2026	High-risk AI systems must be fully compliant
August 2, 2027	Full enforcement for all provisions

1.3 Immediate Actions Required

1. **Inventory all AI systems** currently in use, development, or procurement
2. **Classify each system** according to the risk-based framework
3. **Identify prohibited practices** and cease any non-compliant uses immediately
4. **Prioritize high-risk systems** for compliance assessment
5. **Establish governance** with clear accountability for AI compliance
6. **Engage legal expertise** familiar with EU AI Act requirements

7. **Implement AI literacy training** for staff operating or overseeing AI systems

1.4 AI Literacy Requirement (Article 4)

Since February 2, 2025, providers and deployers must ensure staff have sufficient AI literacy. This means personnel must understand:

- Basic functioning of AI systems they work with
- Capabilities and limitations of those systems
- Potential impact on individuals and rights
- Context-appropriate skills for their role

This obligation applies to **all** AI systems, not just high-risk. Document training provided and competency assessments.

2 Regulatory Scope and Applicability

2.1 Territorial Scope

The AI Act applies to:

- **Providers** placing AI systems on the EU market or putting them into service, regardless of where they are established
- **Deployers** of AI systems located within the EU
- **Providers and deployers** located outside the EU where the output of their AI system is used in the EU
- **Importers and distributors** of AI systems
- **Product manufacturers** placing products with embedded AI on the market

2.2 Material Scope

The regulation covers AI systems defined as machine-based systems designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment, and that infer from inputs to generate outputs such as predictions, content, recommendations, or decisions.

Exclusions:

- AI systems used exclusively for military, defense, or national security purposes
- AI systems used for scientific research and development before market placement
- Personal, non-professional activities
- Free and open-source AI systems (with exceptions for high-risk and prohibited categories)

2.3 Regulatory Roles

Role	Obligations
Provider	Full compliance with all applicable requirements; conformity assessment; CE marking; post-market monitoring
Deployer	Appropriate use; human oversight; monitoring; incident reporting
Importer	Verify provider compliance; ensure documentation availability
Distributor	Verify CE marking; ensure storage and transport conditions
Authorized Representative	Act on behalf of non-EU providers

3 Risk Classification Framework

The AI Act establishes a risk-based regulatory approach with four tiers. Classification determines applicable obligations.

3.1 Prohibited AI Practices (Article 5)

The following AI practices are banned outright within the EU:

1. **Subliminal manipulation:** AI that deploys techniques beyond a person's consciousness to materially distort behavior, causing significant harm
2. **Exploitation of vulnerabilities:** AI that exploits vulnerabilities due to age, disability, or social/economic situation to materially distort behavior
3. **Social scoring:** Evaluation or classification of persons based on social behavior or personal characteristics, leading to detrimental treatment
4. **Predictive policing:** Individual risk assessments to predict criminal offenses based solely on profiling or personality traits
5. **Facial recognition databases:** Untargeted scraping of facial images from the internet or CCTV for database creation
6. **Emotion recognition:** Inferring emotions in workplaces and educational institutions (except for safety or medical purposes)
7. **Biometric categorization:** Categorizing individuals based on biometric data to infer race, political opinions, trade union membership, religious beliefs, sex life, or sexual orientation
8. **Real-time biometric identification:** In publicly accessible spaces for law enforcement (with limited exceptions)

Enforcement: These prohibitions took effect February 2, 2025. Violations carry maximum penalties of €35M or 7% of global turnover.

3.2 High-Risk AI Systems (Article 6 and Annex III)

AI systems are classified as high-risk if they are:

Category A: Safety components of products covered by EU harmonization legislation requiring third-party conformity assessment (e.g., medical devices, machinery, aviation)

Category B: Systems in areas listed in Annex III:

1. **Biometrics:** Remote biometric identification; categorization based on sensitive attributes
2. **Critical infrastructure:** Safety components in road traffic, water/gas/electricity supply, heating
3. **Education:** Determining access to education; evaluating learning outcomes; monitoring prohibited behavior during exams

4. **Employment:** Recruitment; job advertising; application screening; performance evaluation; promotion/termination decisions
5. **Essential services:** Credit scoring; insurance risk assessment; emergency services dispatch
6. **Law enforcement:** Individual risk assessment; polygraphs; evidence reliability; recidivism prediction; profiling
7. **Migration:** Travel document authenticity; application assessment; detection
8. **Justice:** Research and interpretation of facts/law; application of law

3.3 Limited Risk AI Systems (Article 50)

Systems with transparency obligations only:

- Chatbots and conversational AI (users must be informed)
- Emotion recognition systems (subjects must be informed)
- Biometric categorization systems (subjects must be informed)
- Deep fake and synthetic content generators (content must be labeled)

3.4 Minimal Risk AI Systems

All other AI systems. No specific obligations, but voluntary codes of conduct are encouraged.

4 High-Risk AI System Requirements

Organizations deploying high-risk AI must implement the following requirements before August 2, 2026.

4.1 Risk Management System (Article 9)

A continuous, iterative process throughout the AI system lifecycle comprising:

1. **Risk identification and analysis** of known and reasonably foreseeable risks
2. **Risk estimation and evaluation** considering intended and reasonably foreseeable misuse
3. **Risk management measures** to eliminate or reduce risks through design, technical safeguards, training, or information provision
4. **Testing procedures** to ensure risks are adequately managed
5. **Documentation** of all analyses, evaluations, measures, and residual risks

Risks must be assessed against health, safety, fundamental rights, environment, and democracy.

4.2 Data and Data Governance (Article 10)

Requirements for training, validation, and testing datasets:

- Relevant, sufficiently representative, and free from errors
- Appropriate statistical properties for intended purpose and context
- Consideration of characteristics specific to persons/groups on whom system will be used
- Examination for possible biases with mitigation measures
- Data collection and processing compliant with applicable data protection law
- Clear data provenance and preparation procedures documented

4.3 Technical Documentation (Article 11)

Documentation must be prepared before market placement and kept updated. Required elements include:

- General description (intended purpose, provider, version)
- Detailed description of system elements and development process
- Monitoring, functioning, and control mechanisms
- Description of hardware requirements
- Risk management documentation
- Changes made during system lifecycle
- Performance metrics and validation procedures

- Description of input data characteristics

4.4 Record-Keeping and Logging (Article 12)

- Automatic logging of events during system operation
- Logs enabling traceability of system decisions
- Identification of input data for decisions with significant impact
- Protection of logs against unauthorized access and tampering
- Retention for period appropriate to intended purpose (minimum 6 months)

4.5 Transparency and Information (Article 13)

- Clear instructions for use provided to deployers
- Information on provider identity and contact details
- System characteristics, capabilities, and limitations
- Intended purpose and foreseeable misuse scenarios
- Changes over lifecycle and expected performance metrics
- Human oversight measures and procedures

4.6 Human Oversight (Article 14)

Systems must be designed to allow effective oversight by natural persons:

- Enable full understanding of system capabilities and limitations
- Allow detection and correction of anomalies and dysfunctions
- Permit interpretation of outputs with awareness of biases
- Enable override, interruption, or stopping of system operation
- Provide adequate training for human overseers

4.7 Accuracy, Robustness, and Cybersecurity (Article 15)

- Achieve appropriate levels of accuracy for intended purpose
- Ensure robustness against errors, faults, and inconsistencies
- Address reasonably foreseeable conditions of use and misuse
- Implement protection against adversarial attacks and data poisoning
- Maintain performance under evolving environments
- Provide technical redundancy and fail-safe mechanisms

5 General-Purpose AI Models

The AI Act introduces specific requirements for providers of general-purpose AI (GPAI) models, with enhanced obligations for models posing systemic risk.

5.1 All GPAI Models (Article 53)

Providers must:

1. Prepare and maintain **technical documentation** including training and testing processes, evaluation results
2. Provide **information to downstream providers** integrating the model into AI systems
3. Implement **copyright compliance policies**, particularly regarding EU text and data mining opt-outs
4. Publish **sufficiently detailed summary** of training content

5.2 Systemic Risk Models (Article 55)

GPAI models are presumed to have systemic risk if trained using compute exceeding 10^{25} floating point operations. The EU AI Office may also designate models based on capability assessments.

Additional obligations:

1. Perform **model evaluations** including adversarial testing
2. Assess and mitigate **systemic risks**
3. Track, document, and **report serious incidents** to the AI Office and national authorities
4. Ensure adequate **cybersecurity protection**
5. Notify the **EU AI Office** before market placement

5.3 Timeline

GPAI requirements took effect August 2, 2025. Providers had until August 2, 2027 to comply for models already on market.

6 Deployer Obligations

Deployers of high-risk AI systems have distinct obligations from providers. Understanding these requirements is essential for organizations using third-party AI systems.

6.1 General Deployer Obligations (Article 26)

1. **Appropriate use:** Use AI systems in accordance with instructions for use
2. **Human oversight:** Assign competent, trained personnel with authority to override
3. **Input data:** Ensure input data is relevant and representative for intended purpose
4. **Monitoring:** Monitor operation and suspend use if risks emerge
5. **Record-keeping:** Maintain logs automatically generated by the system
6. **Information to workers:** Inform employee representatives and affected workers
7. **Cooperation:** Cooperate with market surveillance authorities

6.2 Fundamental Rights Impact Assessment (Article 27)

Certain deployers must conduct a Fundamental Rights Impact Assessment (FRIA) **before first use**:

Who must conduct FRIA:

- Public bodies deploying high-risk AI
- Private entities providing public services (education, healthcare, social services, housing)
- Deployers using AI for credit scoring of natural persons
- Deployers using AI for life and health insurance risk assessment

Required FRIA contents:

- Description of processes where AI will be used
- Period and frequency of use
- Categories of affected natural persons and groups
- Specific risks of harm to those categories
- Human oversight measures implementation
- Measures to be taken if risks materialize

Note: FRIA may complement existing Data Protection Impact Assessments but has broader scope covering all fundamental rights, not just data protection.

6.3 Serious Incident Reporting (Article 73)

Providers must report serious incidents to market surveillance authorities within strict timelines:

Timeline	Incident Type
Within 2 days	Widespread infringement or serious/irreversible disruption of critical infrastructure
Within 10 days	Death of a person
Within 15 days	All other serious incidents (serious harm to health, fundamental rights, property, environment)

Deployer obligation: Inform the provider immediately (within 24 hours) upon identifying a serious incident.

Initial incomplete reports are permitted to meet deadlines, with complete reports to follow.

7 Conformity Assessment and Enforcement

7.1 Conformity Assessment (Article 43)

High-risk AI systems must undergo conformity assessment before market placement:

Internal control: Self-assessment based on Annex VI procedures (for most Annex III systems)

Third-party assessment: Required for:

- Biometric identification and categorization systems
- AI systems that are safety components of products requiring third-party assessment
- Systems where the provider has not applied harmonized standards or common specifications

7.2 CE Marking and EU Database Registration (Articles 48, 71)

After successful conformity assessment:

1. Affix **CE marking** to the AI system or accompanying documentation
2. Register in the **EU database** for high-risk AI systems *before* market placement
3. Prepare **EU declaration of conformity** with required attestations

EU Database Registration: Providers must register high-risk AI systems in the publicly accessible EU database, providing system identification, provider details, conformity assessment information, and intended purpose. Registration must occur before placing on market or putting into service.

7.3 Documentation Retention (Article 18)

Providers must retain for **10 years** after the AI system is placed on market:

- Technical documentation
- Quality management system documentation
- Conformity assessment documentation
- EU declaration of conformity
- Changes approved by notified bodies (if applicable)

7.4 Authorized Representatives (Article 22)

Non-EU providers must appoint an authorized representative established in the EU *before* placing high-risk AI systems on the market. The representative must have written mandate to act on behalf of the provider for compliance purposes.

7.5 Market Surveillance (Article 74)

National market surveillance authorities have powers to:

- Request information and documentation from providers
- Access AI systems, data, and source code
- Conduct unannounced inspections
- Order corrective actions or market withdrawal
- Impose penalties for non-compliance

7.6 Penalties (Article 99)

Violation	Maximum Penalty
Prohibited AI practices	€35M or 7% turnover
High-risk system non-compliance	€15M or 3% turnover
Incorrect information to authorities	€7.5M or 1% turnover

For SMEs and startups, the lower of the fixed amount or percentage applies. Member states may impose additional administrative fines.

8 Implementation Roadmap

8.1 Phase 1: Assessment (Months 1-2)

Objective: Understand current state and compliance gap

- Create comprehensive inventory of all AI systems
- Classify each system according to risk framework
- Identify prohibited practices requiring immediate cessation
- Assess organizational readiness for compliance
- Estimate resource requirements and budget
- Engage external expertise as needed

8.2 Phase 2: Design (Months 2-4)

Objective: Establish governance framework and compliance approach

- Establish AI governance structure with clear accountability
- Define policies for AI development, procurement, and use
- Design control frameworks aligned to requirements
- Create documentation templates and processes
- Develop training programs for relevant personnel
- Identify technical solutions for logging, monitoring, and oversight

8.3 Phase 3: Implementation (Months 4-7)

Objective: Deploy compliance controls

- Implement risk management systems for high-risk AI
- Deploy technical documentation processes
- Enable automatic logging and record-keeping
- Implement human oversight mechanisms
- Establish post-market monitoring procedures
- Conduct conformity assessments
- Train operators and overseers

8.4 Phase 4: Operate (Ongoing)

Objective: Maintain compliance and continuous improvement

- Monitor systems for compliance drift
- Conduct regular internal audits
- Update documentation as systems evolve
- Report incidents to authorities as required
- Track regulatory developments and guidance
- Respond to market surveillance activities

9 January 2026 Developments

9.1 Upcoming Deadline: February 2, 2026

The European Commission must publish guidelines on the practical implementation of Article 6 (high-risk classification) by February 2, 2026. This will include:

- Comprehensive list of practical examples of high-risk and non-high-risk AI use cases
- Template for post-market monitoring plans (implementing act)
- Clarification on classification edge cases

Organizations should monitor for these guidelines to inform their risk classification decisions.

9.2 Digital Omnibus Proposal

The European Commission published a proposal in November 2025 to simplify regulatory reporting requirements across the AI Act, GDPR, NIS2, DORA, and Data Act. Key implications:

- Unified incident reporting mechanism across regulations
- **Potential timeline extension:** High-risk compliance linked to standards availability
- Long-stop dates: December 2, 2027 (Annex III systems) and August 2, 2028 (product-embedded)

Status: Under legislative review. Organizations should continue August 2026 preparations but monitor for formal adoption.

9.3 Harmonized Standards Progress

The first draft harmonized standard, prEN 18286 (AI Quality Management Systems), entered public enquiry in October 2025. Key developments:

- **QMS Standard (prEN 18286):** Public enquiry completed, awaiting final publication
- **Risk Management Standard:** Expected to follow in early 2026
- **Accelerated timeline:** CEN-CENELEC adopted exceptional measures for Q4 2026 delivery
- Standards remain voluntary but provide presumption of conformity

9.4 AI Regulatory Sandboxes

Each Member State must establish at least one AI regulatory sandbox by August 2, 2026. The Commission published a draft implementing act on sandbox frameworks in late 2025. Benefits for participants:

- Controlled environment for testing innovative AI systems
- Regulatory guidance during development phase
- Potential reduced compliance burden for sandbox participants

9.5 Code of Practice: AI-Generated Content

The first draft of the Code of Practice on AI-generated content labeling was published December 17, 2025. Final version expected by June 2026. Requirements include:

- Machine-readable watermarking for synthetic media
- Clear disclosure format and placement standards
- Consumer-facing labeling requirements

Hyperion Consulting

hyperion-consulting.io | contact@hyperion-consulting.io