EU ARTIFICIAL INTELLIGENCE ACT (Important Articles)

CHAPTER 1 — General Provisions

Article 1 — Subject Matter

- Purpose is to oversee and establish foundations for human-centric AI that protects health, safety, and fundamental rights, including democracy, the rule of law, and environmental protection from the harmful effects of AI, while supporting innovation.

- Regulation applies to the placing of AI systems on the market, their deployment, and their use.

- Prohibition of certain AI practices and specific requirements for high-risk AI systems, along with obligations for operators.

- Transparency rules for certain systems.

- Harmonised rules for the market placement of general-purpose AI (GPAI).

- Rules on market monitoring, market surveillance, governance, and enforcement.

- Measures to support innovation, focusing on SMEs and startups.

- Regulation applies to:

    - Providers implementing GPAI or AI models in the market, regardless of where they are based.

Article 2 — Scope

This section explains the general points and purpose of the article. It also defines who the regulations apply to.
The article aims to maintain human-centric values in AI law and establish regulatory requirements primarily for providers and operators.

Additional Scope Notes (Continued from Article 2)

- Deployers of AI systems, whether inside their institution or within the EU.

- Deployers outside the EU who make their AI systems available within the EU.

- Importers and distributors.

- Product manufacturers using AI or placing AI systems on the market together with their own products under their own name or trademark.

Exemptions

- These regulations do not apply to AI systems used for military, defense, or national security purposes, nor for police, courts, or other public authorities performing sovereign tasks.
- The Act does not impose regulations on foreign public authorities as long as they safeguard basic human rights.
- Rules do not apply to AI systems built solely for research, testing, or experimental purposes.
- Testing and training AI models do not need to comply with the regulation during controlled testing phases. Testing in real-world situations is also excluded.
- Does not apply to individuals or deployers using AI for purely personal, non-professional activity.
- Does not apply to free or open-source AI unless it is classified as high-risk.

Article 3 — Definitions

(Section not detailed in notes, but refers to key legal definitions used throughout the Act.)

Article 4 — AI Literacy

- Providers and deployers must take appropriate measures to ensure that they and their employees have the necessary level of AI literacy to safely handle and legally operate AI systems.

Summary Note

The rules mainly apply to providers distributing commercial AI systems into the market. Personal, non-commercial, and research use does not fall under these regulations.

Article 7 — Amendments to Annex III

- AI systems must not be able to be exploited due to a person’s status, authority, level of knowledge, economic or social circumstances, or age.

Article 8 — Compliance with the Requirements

- Providers are responsible for ensuring compliance through appropriate and necessary testing and reporting processes.

Article 9 — Risk Management System

- A high-risk management system must be deployed that operates throughout the entire lifecycle of the AI system, with regular systematic review and updates.
- The system must identify future risks the AI may cause to health, safety, or fundamental rights. It must evaluate risks that may emerge over time.
- It must assess risks arising from data collection.
- The system should focus only on risks that can actually be reduced, and address residual risk by designing better software or processes and providing deployers with adequate instructions suited to their technical skill level.
- Testing of high-risk AI systems may include real-world scenarios.
- Results must assess whether the AI system is likely to have an adverse impact on vulnerable groups.

Article 10 — Data and Data Governance

- High-quality datasets must be used for training and testing. Bias and gaps in datasets must be checked.
- Sensitive data can only be used for detecting and correcting bias if no other alternative exists, and must be deleted once used.
- Data used for validation and testing must be accurate and free from bias.

Summary Note

To reduce the risks of high-risk AI systems, risk management systems must detect both current and future problems. Testing can be performed in real-world environments. Datasets must be accurate, unbiased, and suitable for training, validation, and testing.

Article 7 — Amendments to Annex III

- AI must not be able to be exploited on the basis of status, authority, level of knowledge, economic or social circumstances, or age.

Article 8 — Compliance with the Requirements

- Providers are responsible for compliance through appropriate and necessary testing and reporting processes.

Article 9 — Risk Management System

- A high-risk management system must be deployed that runs throughout the entire lifecycle of the AI system, with regular systematic review and updating.
- The system must identify future risks the AI could cause to health, safety, or fundamental rights, and evaluate risks that may emerge.
- Includes evaluation of risks arising from data collection.
- Focuses only on risks that can be reduced, and works to minimise residual risk by improving software or processes and giving deployers clear instructions that match their technical skill level.
- Testing of high-risk systems may include real-world scenarios.
- Results should assess whether the AI system is likely to have an adverse impact on vulnerable groups.

Article 10 — Data and Data Governance

- High-quality datasets must be used for training and testing. They must be checked for bias and gaps.
- Sensitive data can only be used to detect and correct bias if no alternative exists, and must be deleted once used.
- Data used for training, validation, and testing must be accurate and free from bias.

Summary Note

To address risks in high-risk AI systems, a risk management system must be deployed to detect current and future problems. Testing may be carried out in real-world environments. Datasets must be accurate, unbiased, and suitable for training, validation, and testing.

Article 11 — Technical Documentation

- Before a product is launched, technical documentation must be prepared and kept updated.

- SMEs and startups may have a simplified process.

Article 12 — Record Keeping

- High-risk AI systems must be able to automatically record events throughout their lifecycle.
- This allows traceability of the system’s actions and supports accountability.

Article 13 — Transparency and Provision of Information to Deployers

- High-risk AI systems must be transparent, and those using them must understand them correctly and be aware of all associated risks.

Article 14 — Human Oversight

- AI systems must be designed with human–machine interface tools to enable proper monitoring and minimize safety risks.
- The system must be provided in a way that allows the overseer to understand its capabilities and avoid over-reliance.
- For certain high-risk AI systems, any action based on system identification must be verified by at least two competent individuals.

Article 15 — Accuracy, Robustness, and Cybersecurity

- High-risk AI systems must be designed to ensure accuracy, robustness, and security.
- Feedback loops must be monitored and controlled to prevent bias.
- Systems should have backup plans and be secure against third-party exploitation.

Summary Note

High-risk AI systems must simplify the process of human oversight and have fail-safe mechanisms in place.
Users must be informed of all risks.
High monitoring and human supervision are essential to keep systems in check.

Article 16 — Obligations of Providers of High-Risk AI Systems

- Providers must ensure that AI systems meet the required standards.
- A quality management system must be put in place.
- Providers must prove compliance with EU standards and supply contact information.

Article 17 — Quality Management System

- The system must be documented and include strategies for:
  - Regulatory compliance
  - Design and development procedures
  - Testing and validation processes
  - Technical specifications
  - Data management systems
  - Risk management
  - Post-market monitoring
  - Incident reporting
  - Communication procedures
  - Record-keeping
  - Resource management
  - An accountability framework
- The implementation of these measures should be proportionate to the size of the provider’s organisation.

Article 18 — Documentation and Record-Keeping

- All relevant documentation must be kept for 10 years.

Article 19 — Automatically Generated Logs

- Companies providing high-risk AI systems must keep automatically generated logs.
- These logs must be stored for at least 6 months or longer if required.

Article 20 — Corrective Actions and Duty of Information

- If a high-risk system poses a threat, the provider must fix the issue, stop its use, or recall the system.
- The provider must investigate the cause and inform the relevant authorities.

Article 21 — Cooperation with Competent Authorities

- When requested, companies must provide all information needed to prove that their AI system meets the required standards.
- Information must be presented in clear, understandable language.
- Logs must also be provided if requested.
- All collected information is confidential.

Final Note

Providers must establish internal rules and documentation, stay prepared for audits, and keep proof of all processes.
Information must be explained in simple language so that relevant authorities can easily understand it.

Article 22 — Authorised Representatives of Providers of High-Risk Systems

- High-risk AI system providers from non-EU countries must appoint a representative within the EU.
- The representative is responsible for ensuring that the AI system complies with EU regulations, including record-keeping for 10 years.

Article 23 — Obligations of Importers

- Importers must ensure that the AI system meets all regulations.

- Importers must provide contact details on the system or its packaging.
- Records must be kept for up to 10 years.

Article 24 — Obligations of Distributors

- Distributors have the same obligations as importers, except they are not required to provide contact information.

Article 25 — Responsibilities Along the AI Value Chain

- Anyone who distributes, modifies, or embeds a high-risk AI system is then considered its provider.
- Original providers must still comply unless they forbid high-risk use.

Article 27 — Fundamental Rights Impact Assessment for High-Risk Systems

- Before using a system, an assessment must be conducted on how it might affect people’s fundamental rights.
- The assessment must consider **how and when** the system will be used, **who** it may affect, and **what risks** it may pose.

Article 28 — Notifying Authorities

- All EU member states must assign **at least one authority** responsible for oversight, and they must work together.
- The team should include expertise in IT, AI, and law.

Article 30 — Notification Procedure

- Authorities may only be notified when companies meet certain requirements.
- If no objections are raised, the assessment body can begin its activities.

Article 40 — Harmonised Standards and Standardisation Deliverables

- Requests for standardisation and harmonisation will also include ways to improve AI system performance, such as reducing energy consumption.

- The aim is to promote investment and innovation in AI and increase legal certainty.

Final Note

High-risk AI systems must have human oversight and official representatives who assess risks.
There are many communication frameworks that connect different sectors and professions, and all parties must comply.

Article 44 — Certificates

- Certificates must be written in a language that can be easily understood.

- Certificates are valid for up to five years for certain AI systems, and four years for others.

- They can be extended after re-assessment.

Article 50 — Transparency Obligations

- Companies must inform users when they are interacting with an AI system.

- Synthetic content (such as deepfakes) must be clearly marked as artificially generated.

- Users must be notified when AI is used for emotion recognition or content alteration, unless it is for legal, artistic, or satirical purposes.

Article 51 — Classification of General-Purpose AI Models

- AI models have systemic risk if they have high-impact capabilities, determined by technical tools and benchmarks.

- If a model uses a large amount of computation for training, it may fall under this category.

Article 57 — AI Regulatory Sandboxes

- Member states must create at least one AI regulatory sandbox at a national level.
- Sandboxes allow AI systems to be developed, tested, and validated before release.
- AI systems can use sandbox certification as proof of compliance.

Article 58 — Arrangements for Sandboxes

- Access to sandboxes will be free for small businesses and startups.
- Sandboxes help providers comply with regulation and encourage cooperation.

Article 59 — Personal Data in Sandboxes

- Personal data may be used in a controlled environment only when developing systems for public interest.
- Data must be deleted once testing is complete.

Article 60 — Testing High-Risk AI Systems

- High-risk AI systems can be tested under real-world conditions.
- Testing lasts 6 months + 6 months if needed.
- Test data must be protected.

Final Note

Companies must have the necessary certificates written in simple language.
Regulatory sandboxes will be created for testing, and real-time sensitive data may be used under regulation.
A regulatory committee will be created to oversee this process.

Article 61 — Consent of Participants

- People being tested must be informed about tests and give their consent.
- They must be told about their rights.

Article 62 — Support for SMEs and Startups

- The EU is asking member states to support small and medium-sized businesses and startups in understanding and complying with EU regulations.
- Priority access should be given to regulatory sandboxes.
- The goal is to make it easier for SMEs to participate in the development of AI standards.

Article 67 — Advisory Forum

- An advisory forum must be established to provide technical expertise and guidance to the Board and Commission.

Article 71 — EU Database

- The database will include information on both high-risk and non-high-risk AI systems.
- The database will be publicly available.

Article 72 — Post-Market Analysis

- Systems must collect and analyse performance data throughout the entire lifecycle of AI systems.

Final Note

To promote ethical standards in AI, the EU is prioritising easy access for SMEs and startups so they can contribute to ethical industry standards.
Forums for analysis must be set up, and individuals across different sectors should have access to file opinions and contribute.