REGÉNYI TAMÁS
ÜGYVÉD
JOGI TANÁCSADÁS

EU AI Act Explained

October 14, 2026

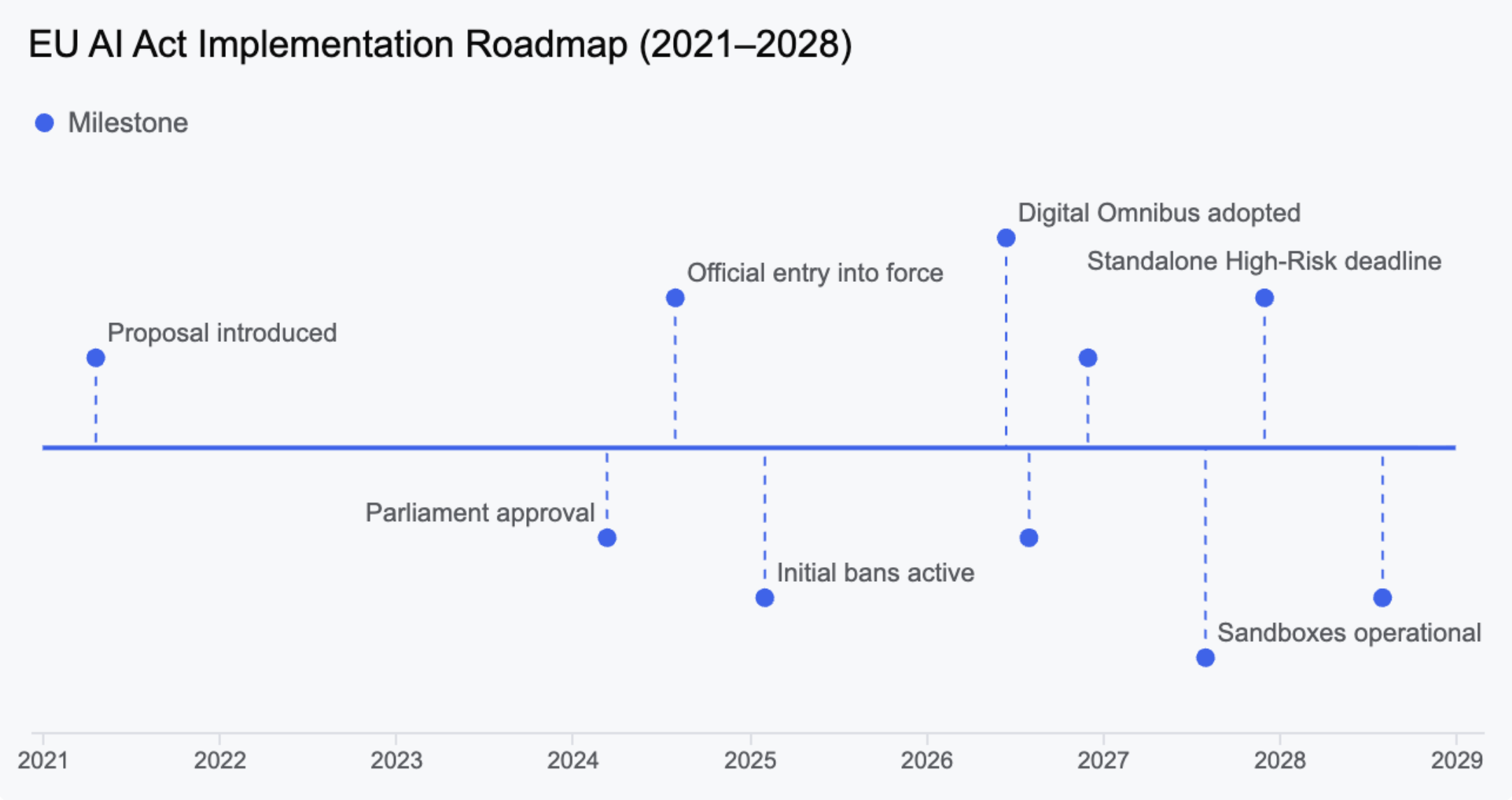
The foundation of the AI Act

- European Parliament voted on in March 2024
- AI act regulation entered into force on August 1, 2024
- Fully active EU regulation across all 27 EU member states.
- Regulation (EU) 2024/1689
- EU is enforcing the AI Act's rules in stages

The Amendment of the AI Act

- Digital Omnibus updates
- Omnibus = "for all" or "including everything” (latin)
- Multiple technical adjustments, corrections, and minor deadline extensions for various digital regulations bundled into a single, comprehensive law. Instead of debating and voting on dozens of separate minor updates, to pass them all at once.
- Voted on in March and June 16, 2026 (423-to-57)
- To fine-tune implementation timelines: new AI Act implementation dates
- Push back high-risk software deadlines to late 2027
- Simplify compliance
- Ban AI tools used to generate non-consensual intimate imagery
- The Omnibus package entered into force on July 27, 2026

EU AI Act Implementation Roadmap



Current law enforcement timelines

REGÉNYI TAMÁS ÜGYVÉD JOGI TANÁCSADÁS

Deadlines	Subject of Compliance
February 2, 2025	**Prohibited AI Practices:** Bans on “unacceptable risk” AI systems social scoring and non-consensual intimate/sexual deepfakes cognitive behavioral manipulation or untargeted scraping of facial images
August 2025 and August 2026	**General-Purpose AI (GPAI) & Transparency:** Obligations for GPAI models Transparency requirements (such as labeling AI-generated content and chatbots) Watermarking and technical documentation.
August 2, 2027	Every member state must have at least one **operational AI Regulatory Sandbox** to let companies safely test software under regulatory supervision.
Postponed to: December 2, 2027	**High-Risk Systems:** For Stand-alone high-risk AI systems listed under Annex III like AI used in critical infrastructure, education, employment screening, biometrics, and law enforcement
Postponed to: August 2, 2028	**High-Risk Systems:** For product-embedded AI obligations regulated under Annex I AI used in health and safety frameworks (medical devices, aviation, automotive)

Risk Tier I: Unacceptable Risk (Outright Banned)

- AI systems that violate EU fundamental rights, exploit human vulnerabilities, or pose a clear threat to safety and society.
- There is no compliance path forward; these tools are strictly illegal in the EU.
- Key Examples:
  - Government-run social scoring systems.
  - Cognitive-behavioral manipulation of vulnerable groups or children.
  - Real-time remote biometric identification in public spaces by law enforcement (with narrow exceptions).
  - Emotion recognition tools used in workplaces and educational institutions.
  - Untargeted scraping of facial images from the internet or CCTV to build databases.
  - Non-consensual sexual/intimate deepfakes ("nudifiers") and untargeted generation of child sexual abuse material (CSAM).
- Enforcement Status: Banned since February 2, 2025 (with deepfake/CSAM additions actively enforced by December 2, 2026).

Risk Tier II: High Risk (Strictly Regulated)

- AI systems that pose significant risks to people's health, safety, or fundamental rights.
- They are legally permitted, but providers and deployers must pass heavy ex-ante (before market entry) and ongoing compliance audits.
- **Annex I Products**: AI that acts as a safety component of a product already regulated under EU safety laws (e.g., medical devices, machinery, toys, aviation, or automotive).
- **Annex III Standalone Systems**: AI deployed in 8 high-impact sectors: biometrics, critical infrastructure, education and vocational training, employment/HR, essential public/private services (e.g., credit scoring), law enforcement, migration/border control, and administration of justice.
- Mandatory Obligations (Chapter III):
  - Robust, continuous risk management systems.
  - High-quality data governance and bias mitigation in training and testing datasets.
  - Automatic event logging and traceability.
  - Clear technical documentation and user transparency.
  - **Effective human oversight interfaces so humans can monitor or override the AI.**
  - A formal conformity assessment (self-check or third-party Notified Body audit depending on the sector).
- Enforcement Status: Postponed via the Digital Omnibus package; takes effect on December 2, 2027 (for Annex III systems) and August 2, 2028 (for Annex I product-embedded AI).

Risk Tier III: Limited Risk / Transparency Risk (Disclosure Duties)

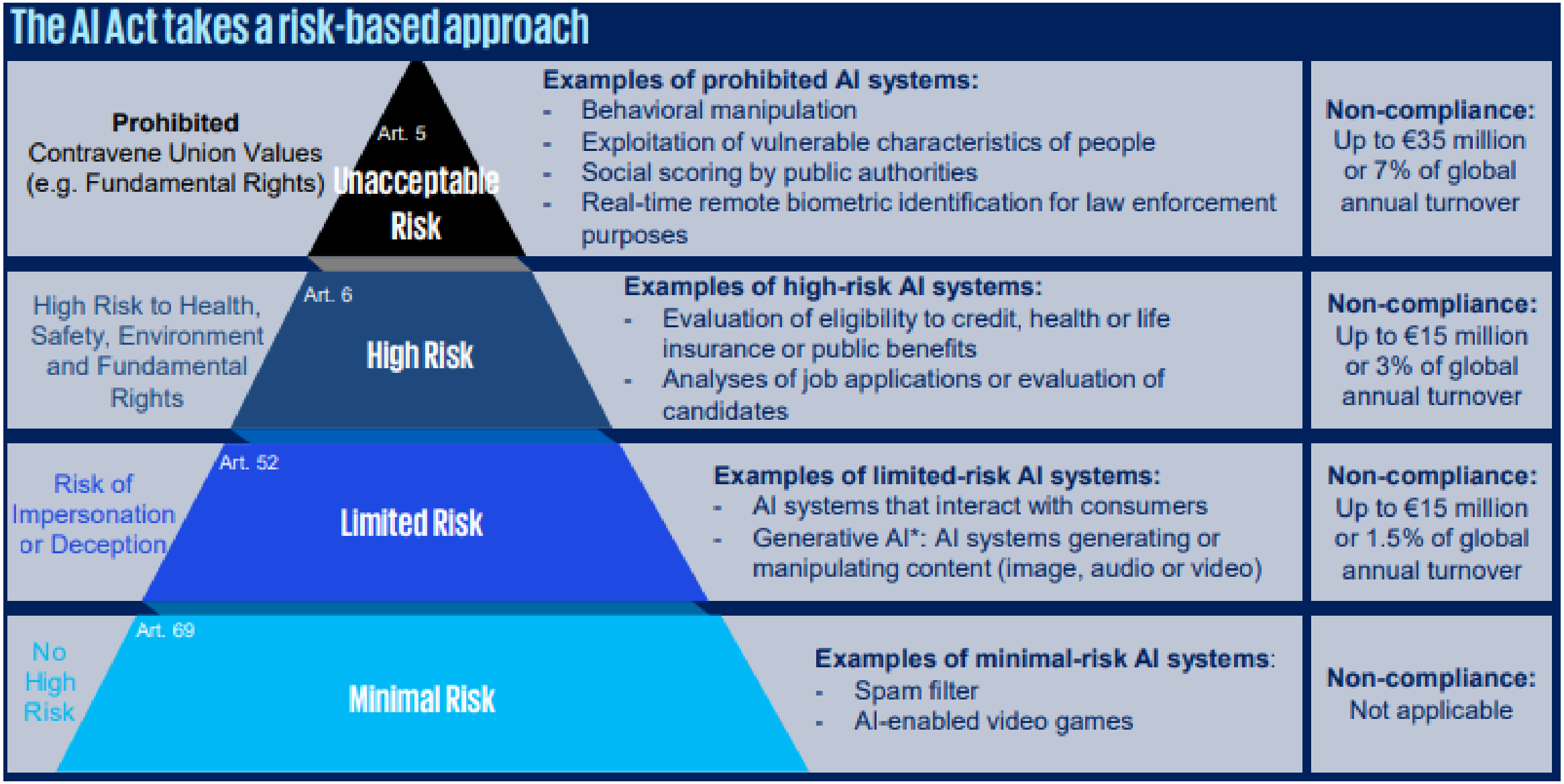
- AI systems that interact directly with humans or generate synthetic content where people have a right to know they are dealing with a machine.
- Key Examples:
  - Chatbots and conversational virtual assistants (users must be informed they are talking to an AI).
  - Emotion recognition or biometric categorization systems not falling under the banned category (must disclose use to individuals).
  - Deepfakes, AI-generated images, audio, or video (must be clearly watermarked or labeled as artificially generated).
  - Generative AI models and General-Purpose AI (GPAI) (require technical documentation, training data summaries, and copyright compliance).
- Enforcement Status: Article 50 transparency obligations took effect on August 2, 2026, with legacy GPAI watermarking deadlines rolling into December 2, 2026.

Risk Tier IV: Minimal or No Risk (Unregulated)

- The vast majority of everyday AI applications that pose little to no threat to human rights or safety.
- Key Examples:
  - AI-powered video games.
  - Spam filters in email clients.
  - Inventory management systems or internal business data analytics tools.
- Mandatory Obligations: None. Developers are encouraged to follow voluntary codes of conduct, but no legal restrictions or compliance burdens apply.

EU AI Act four tier risk levels

REGÉNYI TAMÁS
ÜGYVÉD
JOGI TANÁCSADÁS



The 4 risk levels under the EU AI Act

REGÉNYI TAMÁS
ÜGYVÉD
JOGI TANÁCSADÁS

The EU AI Act's risk-based approach classifies AI systems into categories based on their potential harm to ensure appropriate regulatory measures are applied.

Unacceptable Risk

Definition: AI systems that pose a clear threat to safety, livelihoods, and rights, leading to their prohibition. Ex. Real-time Biometric Surveillance

High Risk

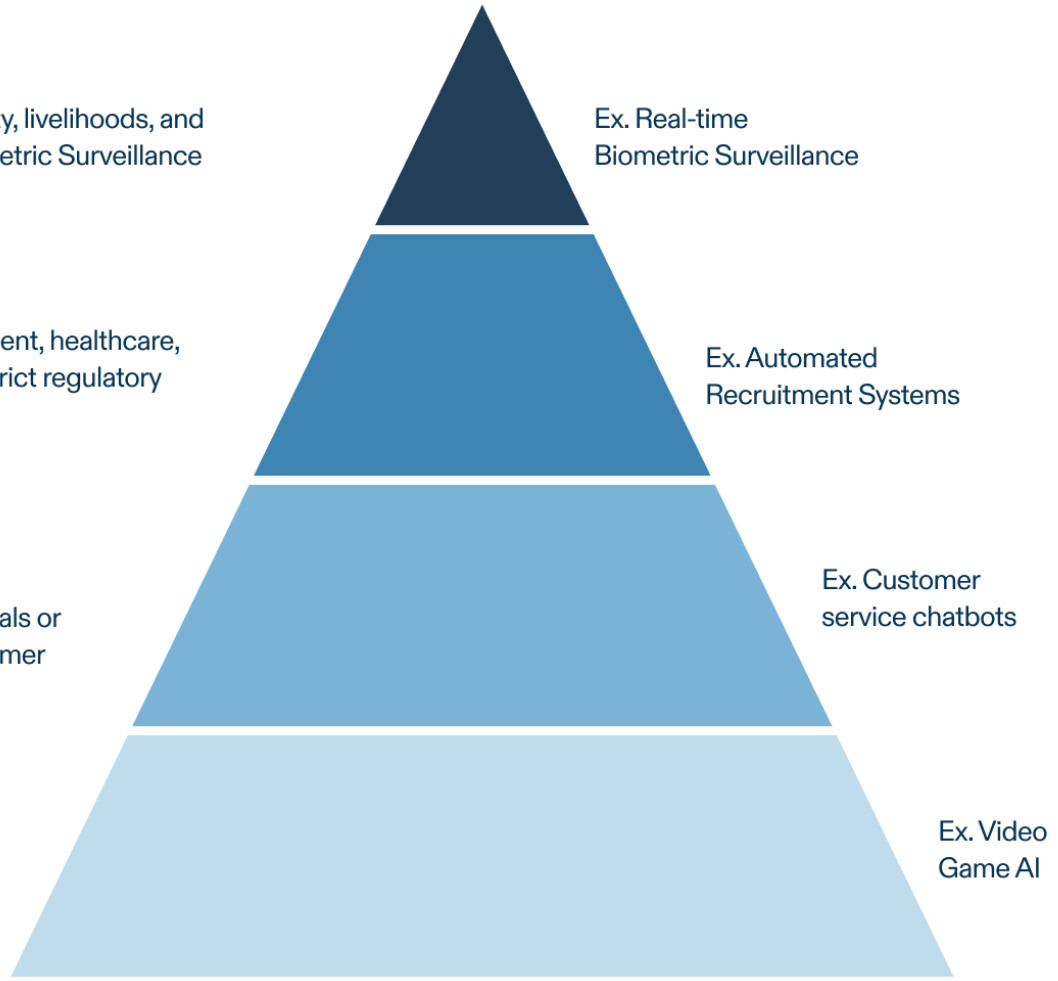
Definition: AI systems in critical sectors like employment, healthcare, and financial services (particularly lending), require strict regulatory compliance. Ex. Automated Recruitment Systems

Limited Risk

Definition: AI systems with limited impact on individuals or society, requiring transparency obligations. Ex. Customer service chatbots

Minimal Risk

Definition: AI systems with minimal or no risk, subject to voluntary codes of conduct and minimal regulatory oversight. Ex. Video Game AI



Penalties for non-compliance with the EU AI Act

- Tiered fine system
  - Article 99 for specific AI models
  - Article 101 for General-Purpose AI models
- Administrative fines based on
- either a fixed maximum euro amount or
- percentage of their **worldwide** annual turnover

Violation Type	Maximum Fixed Fine	Maximum Global Turnover %
Tier 1: Prohibited AI Practices (Article 5) (e.g., social scoring, untargeted facial scraping, manipulation)	Up to €35 million	Up to 7%
Tier 2: High-Risk AI & Operator Duties (e.g., data governance, risk management, transparency breaches)	Up to €15 million	Up to 3%
Tier 3: Misleading or Incorrect Information (e.g., providing false data or withholding info during audits)	Up to €7.5 million	Up to 1%

Financial sector regulations: Dual Compliance Burden

- Digital Operational Resilience Act (DORA) regulates financial sector resilience
- AI-driven systems are subject to both
  - AI-specific risk management rules (AI Act) and
  - Financial sector resilience requirements (DORA).
- Financial firms using AI-powered trading, fraud detection, risk assessment, and cybersecurity tools must comply with both legal acts.
- The AI Act classifies credit scoring, financial risk assessment, fraud detection, anti-money laundering (AML), automated trading, and investment decision-making AI systems as “high-risk”
- AI-driven financial tools must comply with AI Act obligations (transparency, bias mitigation, accuracy testing etc.) and DORA’s ICT risk management standards.
- DORA requires financial institutions to assess third-party ICT service providers (including AI providers).
- Banks and insurers must ensure AI vendors comply with both the AI Act and DORA.

EU AI Act regulation for Digital Medicine in tissue diagnostics

- AI applications in digital pathology as "High-Risk AI Systems ”
- the vast majority of AI used to analyze whole-slide images (WSIs), diagnose diseases, or support clinical decisions
- AI in digital pathology is classified as high-risk because it directly affects **patient diagnoses**, **treatment plans**, and **human health outcomes**, qualifying automatically through its status as a regulated medical device.

The High-Risk Classification Pathway (Article 6 & Annex I)

Under Article 6(1) and Annex I, an AI system is automatically considered high-risk if

- it is a product—or a safety component of a product—covered by EU harmonization legislation and
- requires a third-party conformity assessment.
- The IVDR/MDR Link: Digital pathology software typically functions as **Software as a Medical Device (SaMD)**. Because diagnostic pathology tools fall under the In Vitro Diagnostic Medical Devices Regulation (IVDR) or Medical Devices Regulation (MDR) (usually as Class IIa or higher, or Class C/D under IVDR), they are governed directly by this high-risk classification.
- The Compliance Timeline: Following the Digital Omnibus package, the compliance deadline for these Annex I embedded medical AI systems has been set to August 2, 2028. This provides developers time to align the AI Act requirements directly with their existing IVDR/MDR CE-marking technical documentation.

Core Requirements for Medical Device AI Providers (Chapter III)

Chapter III (Sections 1–3) imposes strict, binding obligations that must be designed into the software lifecycle:

- **Data Governance & Bias Mitigation (Article 10)**: Training, validation, and testing datasets must be subject to high quality-governance practices. For pathology, this mandates evaluating datasets for data-provenance, demographic or technical bias, and ensuring that training data accounts for variation across different slide scanners and staining techniques.
- **Technical Documentation & Logging (Articles 11 & 12)**: Systems must automatically record logs throughout their operation to ensure traceability, auditable performance tracking, and detection of performance drift over time.
- **Transparency & Explainability (Article 13)**: The software must be designed to deliver interpretable outputs. The user interface must clearly state the system's level of accuracy, specifications, and potential limitations to the practicing pathologist.
- **Human Oversight (Article 14)**: The tool must allow a human professional to fully supervise, override, or disregard the AI's conclusions. In digital pathology, this means the software must function strictly to assist the pathologist, ensuring the definitive diagnostic validation remains completely with the human physician.
- (e.g., automated cell counting, tumor grading, or metastasis detection)

Obligations for Deployers (Laboratories & Hospitals)

The AI Act doesn't just regulate developers; it places explicit legal obligations on the healthcare organizations and pathology laboratories that deploy the software:

- **AI Literacy (Article 4)**: Labs must ensure that their personnel (pathologists, lab technicians) possess the necessary training to interpret the software outputs and understand its limits.
- **Post-Market Surveillance & Incident Reporting**: Hospitals must monitor the AI system in real-world clinical application and immediately report any serious adverse diagnostic incidents or algorithmic anomalies to both the provider and the market surveillance authority.

Core Reasons for High-Risk Classification

- **Direct Impact on Patient Outcomes**: Pathology AI analyzes tissue samples to detect cancer, grade tumors, or identify life-altering diseases. An algorithmic error or false negative can delay critical treatment, while a false negative or false positive can lead to unnecessary, invasive medical procedures.
- **Article 6 and Annex I of the AI Act:** any software that functions as a medical device or a safety component under the EU Medical Devices Regulation (MDR) or In Vitro Diagnostic Regulation (IVDR) requires a third-party safety check. This automatically groups diagnostic pathology software into the high-risk category.
- **Algorithmic Black-Box Complexity:** Deep learning models process complex, high-resolution whole-slide images using math patterns that are hard for human experts to trace. If a model reaches a wrong conclusion, understanding why it failed can be difficult without strict transparency and data logging.
- **Technical and Environmental Drift:** Staining variations between laboratories, different slide scanner hardware, or changes in tissue preparation can cause an AI model's performance to degrade. Without constant post-market monitoring, small technical shifts can cause major diagnostic mistakes in real-world hospital use.

The outcome for Digital Medicine in tissue diagnostics

- Digital Pathology AI system remains classified as **High-Risk**, even if a pathologist must validate every single output and studies show the AI outperforms human doctors
- the presence of human verification and excellent standalone accuracy does not lower a system's risk tier. Here is why the law treats it this way:
    1. Human Oversight is a Requirement, Not an Exemption
    2. The Legal Trigger: The IVDR / MDR Link
    3. Highly Accurate AI Still Needs Strict Regulation

Human Oversight is a Requirement, Not an Exemption

The AI Act does not view the pathologist's final sign-off as a reason to exempt the software.

The "Human Oversight" **(Article 14)** is a mandatory rule that high-risk AI must satisfy.

- The law intentionally builds in the pathologist as a safety check to prevent over-reliance on the machine.
- Even though the pathologist influences the final outcome, the software remains high-risk because it is **the tool driving, guiding, and heavily influencing that doctor's clinical decision**.

The Legal Trigger: The IVDR / MDR Link

The risk classification is determined by what the software does, not how accurate it is or who looks at it.

- Digital Pathology AI analyzes tissue to assist in diagnosing diseases like cancer, it is regulated under the EU In Vitro Diagnostic Regulation (IVDR) or Medical Devices Regulation (MDR).
- Article 6 of the AI Act explicitly states that if a piece of software is covered by these medical regulations and requires a third-party safety check (a Notified Body audit), it is automatically High-Risk.

Highly Accurate AI Still Needs Strict Regulation

Even if clinical studies prove that an AI system performs better or more consistently than an average pathologist, the EU enforces high-risk rules to protect against specific hidden failures:

- **Automation Bias:** Studies show that when an AI is highly accurate, human doctors naturally drop their guard. Pathologists may start blindly trusting **("rubber-stamping"**) the AI's suggestions, effectively neutralizing the human safety check.
- **The "Black Box" Problem:** If the AI is incredibly smart but cannot explain why it flagged a specific cluster of cells, the pathologist cannot safely validate it. The AI Act's high-risk rules force developers to **make the AI transparent and explainable**.
- **Dataset Bias & Technical Drift:** An AI might perform perfectly in a published study using images from a specific high-end scanner. However, if a hospital deploys it using a different slide scanner or a slightly different tissue staining technique, **the accuracy can drop drastically**. The high-risk framework mandates strict data governance and post-market tracking to catch these variations.

Key Enforcement Rules & Protections

- The Higher-Of Rule (vs. Lower-Of Rule):
  - For standard enterprises: whichever is higher, the flat euro amount / the global turnover percentage.
- Protections for SMEs and Start-ups (Digital Omnibus updates):
  - whichever amount is lower, shielding smaller operations from total financial ruin.
- General-Purpose AI (GPAI) Penalties (Article 101):
  - Directly fine foundational AI model providers (Tier 2 fine)
  - for intentional or negligent infringements, information failures, or refusing model access.
- Market Withdrawal and Bans (Beyond financial penalties):
  - National market surveillance authorities hold the power to order
  - immediate stop, recall, or permanent EU-wide ban of non-compliant AI systems.
- Extraterritorial Reach ("long-arm provision"):
  - to any developer, importer, or deployer outside the EU
  - whose AI systems or outputs are placed on or affect the European market.

non-EU companies

- If they meet either of these criteria:
  - Placing on the Market:

    Making AI system or General-Purpose AI (GPAI) model available for distribution or use on the EU market

    (e.g., a U.S. SaaS company selling to French clients).
  - Output Used in the EU:

    Even if hosted entirely outside of Europe,

    If the outputs generated by the AI are used inside the EU

    (such as data predictions, generated text, images, or automated decisions
- Who Enforces the Rules ?
  - The EU AI Office: Central monitoring large GPAI foundational models, right to demand information, conduct remote model evaluations, and mandate strict risk mitigation measures.
  - National Competent Authorities: Market Surveillance Authorities to police localized AI systems.

Enforcing Penalties Across Borders

- **Mandatory Authorized Representatives**:
  - Located physically within the EU,
  - Acts as the legal proxy, housing technical documentation and
  - Serving as the direct point of contact for regulators facing enforcement actions.
- **International Trade and Market Bans**:
  - EU AI Office can issue a permanent EU-wide digital block or physical market ban,
  - App stores, cloud hosting providers, and European infrastructure partners:
  - will be ordered to halt the distribution of that AI service within the 27 EU nations.
- **The "GDPR Model" Precedent**:
  - Cooperation with global regulatory allies,
  - Cross-border corporate agreements, domestic collection practices, and
  - Asset freezes on international subsidiaries

Sources

- https://artificialintelligenceact.eu/
- https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- https://pmc.ncbi.nlm.nih.gov/articles/PMC13053491/
- https://health.ec.europa.eu/medical-devices-sector_en
- https://www.sciencedirect.com/science/article/pii/S0168851024001623