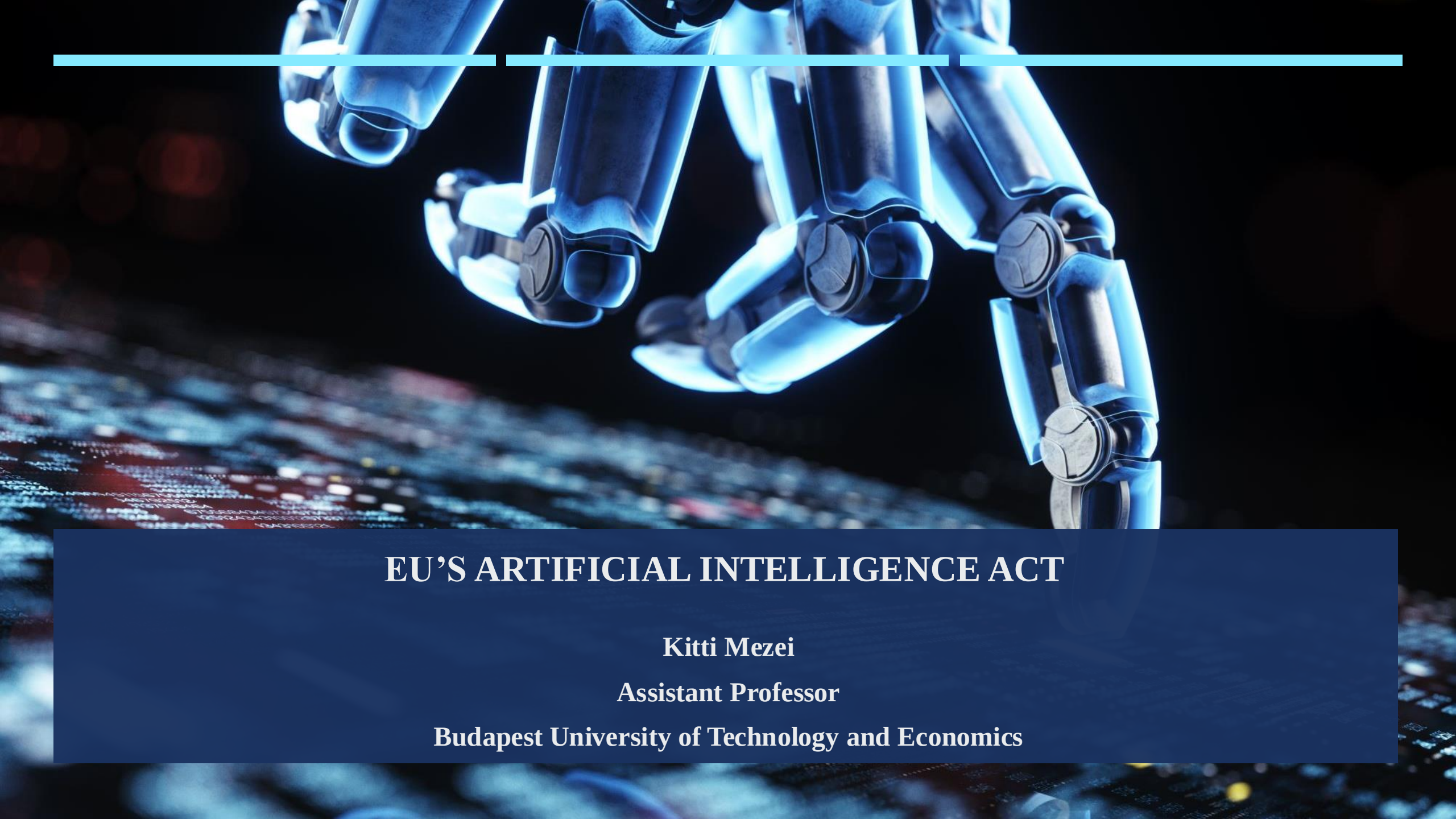


EU’S ARTIFICIAL INTELLIGENCE ACT

Kitti Mezei

Assistant Professor

Budapest University of Technology and Economics

AI ACT

- The EU AI Act is a landmark regulation, representing a significant step towards the legal governance of AI technologies.
- The AI Act came into effect on August 1, 2024, and aims to comprehensively and generally regulate AI systems used in the EU and address associated risks.
- Although referred to as an "Act," it is formally an EU Regulation (Regulation EU 2024/1689), ensuring uniform application across member states, directly enforceable.
- The AI Act will be implemented gradually (2025–2027), allowing market participants to prepare.
- The AI Act applies to providers placing AI systems in the EU market, users within the EU, and also outside providers/users if their AI system outputs are used in the EU (extraterritorial scope).

AI ACT

- The EU AI Act's recitals lay out its foundational principles and objectives. These include:
  1. ensuring AI systems' safety and respect for fundamental rights (human-centred),
  2. promoting AI innovation and uptake within the EU;
  3. creating legal certainty to facilitate investment and innovation in AI; and
  4. addressing risks associated with specific uses of AI, particularly those posing high risks to fundamental rights.

AI ACT

- Prohibited AI Practices – February 2, 2025
- Specific obligations for general-purpose AI models – August 2, 2025
- Most obligations, including the rules for high-risk AI systems defined in Annex III and specific transparency requirements – August 2, 2026
- Rules for high-risk AI systems defined in Annex I – August 2, 2027

AI SYSTEM

'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Example: AI-Based Medical Image Analysis

Many hospitals and healthcare providers use AI systems to assist doctors in analyzing images such as X-rays, CT scans, and MRIs. These systems are trained on labeled medical image datasets to recognize patterns and identify potential abnormalities.

- **Machine System**: A computer program, software.
- **Input Processed**: Analysis of medical images.
- **Conclusion**: Identifies patterns in the images that may indicate diseases or abnormalities.
- **Autonomy**: Highlights potential problem areas in the images, supporting doctors in making more informed diagnoses.

AI LITERACY

Article 4

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

SECTOR-SPECIFIC REGULATION

- **The AI Act shares its legal framework and significance with other critical EU regulations:**
  - EU Medical Device Regulation (MDR)
  - In Vitro Diagnostic Medical Devices Regulation (IVDR)
  - Clinical Trials Regulation (CTR)
  - General Data Protection Regulation (GDPR)
- These regulations have already influenced the governance of regulated digital medical products, setting a precedent for AI systems.
- Unlike sector-specific which regulate specific products like medical devices, the AI Act covers a wide range of AI applications.
- The AI Act addresses general AI-related risks (bias and explainability etc.) and ethical considerations (fairness and transparency etc.) across industries, beyond just market access, safety, and effectiveness.

REGULATION FOR DIGITAL MEDICAL PRODUCTS

Pivotal Regulation for Digital Medical Products:

- Covers all AI/ML-enabled medical devices and systems, including:
  - Stand-alone software as medical devices (SaMD).
  - AI as medical devices (AIaMD).
  - Complex hardware-software combinations used in diagnostics and clinical support.

Aligns with existing EU MDR and IVDR, which already enforce stringent sector-specific regulations for market access, safety, and compliance.

Intersection with GDPR:

- Many digital medical products process personal health data, requiring compliance with the GDPR alongside AI Act obligations.
- Adds another layer of regulatory scrutiny for data protection, security, and transparency.

RISK-BASED APPROACH

- **Prohibited AI** (e.g., social credit scoring for health benefits)
- **High-risk AI systems**
  - AI-based medical devices falling within the scope of MDR (e.g., AI Clinical Decision Support Systems);
  - AI for risk assessment and pricing for health insurance;
  - AI for evaluating and classifying emergency calls; AI for decisions on dispatching medical aid;
  - AI for emergency healthcare patient triage systems;
  - AI used by public authorities to evaluate eligibility for essential public assistance benefits and services, including healthcare services.
- **Low-risk AI systems** (AI-chatbots providing advice on wellbeing; AI-based food intake sensors in home care settings; AI-generated medical deepfakes, e.g., adding and eliminating tumours from medical images.
- **No risk AI systems** (AI-based systems used for administration in healthcare, which do not serve a purely medical purpose)
- **General-purpose AI and foundation models** (e.g., generative AI, LLMs to take clinical notes)

HIGH-RISK AI SYSTEMS

- AI systems in regulated digital medical products, such as those in AI/ML-enabled medical devices, are classified as “high-risk” (Art. 6, Annex II).

- **Compliance requirements**
- **Risk management processes** must align with both the EU MDR and the AI Act: Identify, evaluate, and mitigate reasonably foreseeable risks to health and safety, fundamental rights, such as privacy and data protection (Article 9).
- **Data quality and governance requirements** beyond GDPR: emphasize training, validation, and testing datasets; assess data availability, quantity, and suitability; examine data for biases that could affect health and safety; tailor systems to the specific geographical, contextual, behavioral, or functional settings of use (Article 10).
- **Detailed technical documentation** must be attached (Article 11).
- Systems for **record-keeping and automated logging events** must be implemented (traceability) (Article 12).
- Must operate **transparently** (instructions for use) (Article 13).
- **Human oversight** and the ability for intervention must always be maintained (ensure safe and ethical use) (Article 14).
- Must meet accuracy, robustness, and **cybersecurity standards** (Article 16)
- **Quality management systems** (Article 17) (manufacturers of regulated medical devices typically use ISO/IEC 13485)
- **Human rights impact assessment** (Article 27).

- **Post-market monitoring, reporting serious incidents, internal and external audits, cooperation with competent authorities.**

HIGH-RISK AI SYSTEMS

Technical Documentation Mandate:

- Required for all high-risk AI systems, including minor sub-components of regulated digital medical products (Article 11).
- Demonstrate compliance with the AI Act before the system is placed on the market or put into service. Must be completed, updated, and maintained over the system's lifecycle.

Key elements include:

- **System Elements and Development Process:** Design specifications, system architecture, key design choices, rationale, and assumptions.
- **Data Requirements:** Training methodologies, computational resources, and data sets used.
- **Validation and Testing:** Procedures, performance metrics, and results.
- **Lifecycle Management:** Requirements for accuracy, robustness, cybersecurity, and resilience.
- **Integration with EU MDR/IVDR Technical Documentation:** Regulated products must provide Annex IV documentation for the AI system in addition to the MDR/IVDR documentation. Article 11(2) allows creation of a single technical documentation file: Combines AI-specific and medical device requirements for efficiency. Leverages existing MDR/IVDR documentation, appending AI-specific information.
- **Support for SMEs and Start-Ups:** the AI Act allows simplified documentation for SMEs and start-ups.

HIGH-RISK AI SYSTEMS

- The AI Act adds new requirements specifically for AI medical devices. These are in addition to the MDR.

- **Third-Party Conformity Assessment:**
  - AI medical devices must undergo the regular MDR conformity assessment, which includes third-party evaluation.

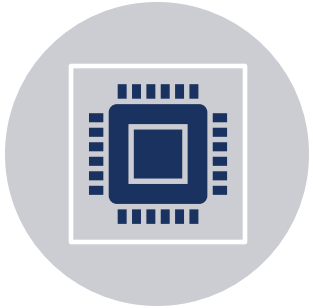
- **Integrated Compliance:**
  - The AI-specific requirements will be integrated into the MDR conformity assessment process, creating a dual-layered regulatory framework.

HIGH-RISK AI SYSTEMS

- **Obligations for High-Risk AI Systems:**
- Providers, importers, distributors, and deployers must ensure compliance throughout the AI lifecycle (Articles 16–29).

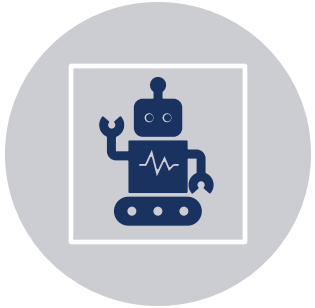
- **Responsibilities include:**
  - Maintaining high standards of conformity (Article 48).
  - Ensuring proper CE marking (Article 49).
  - Registering systems and maintaining data in the EU Database for High-Risk AI Systems (Article 51).

CHALLENGES



Overlap with MDR/IVDR:

Medical AI developers must comply with both EU MDR and AI Act, leading to potential confusion over overlapping requirements.



General-purpose AI models (e.g., LLMs) integrated into medical devices blur the lines between AI Act and MDR compliance.

Example: Using a general AI (e.g., LLM) as a subsystem in a medical AI device for natural language output.

Regulatory uncertainty: Determining intended use and compliance obligations when general AI and medical AI converge.

SMEs face higher costs and resource challenges, with additional burdens.