holi food

Funded by the European Union

The AI Act and Food Safety (Research)

Safe Food, Smart Future: European Innovations for a Changing World

UNIVIE, Eva Korenjak Lalovic

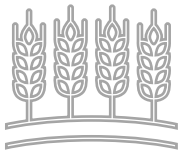
Final conference of the HOLiFOOD and FoodSafeR projects, Wageningen, NL,10 June 2026

Agenda

1. AI in Food Safety
2. AI Act – an Overview
3. AI Act and Food Safety
4. Conclusion, Q & A

AI in Food Safety

- Most **current** approaches **fragmented**, **reactive** and **symptoms based** (i.e., presence of a hazard)
- **AI** (machine learning, computer vision, natural language processing, auditory recognition) can process **large volumes** of data from **different sources** → enables shift to **proactive**, more **effective** and **accurate** risk management
  - supply chain monitoring (traceability, food waste reduction)
  - contamination detection
  - predictive analytics (forecasting of foodborne illness outbreaks)
  - inspection and compliance, consumer safety and livestock health management



- While promising, AI introduces **risks and uncertainty** related to system complexity, autonomy, and reliability

holi food

AI Act – an Overview

- first-ever comprehensive legal framework on AI worldwide
  - **binding** and **directly applicable**
  - "product safety regulation"
  - **trustworthy** AI in the EU → safety, fundamental rights and human-centric AI
- subject matter: **development** & **use** of AI systems → obligations for **developers** and **deployers**
  - Providers in EU (established in EU or in thrid country)
  - Users (established / located in the EU)
  - E.g. AI system developed outside of EU and provided by non-EU entity with outputs in the EU → AI Act applies (extraterritorial effect)
- **risk-based** approach → prohibitions, requirements based on the (likelihood of) harms

holi food

AI Act – an Overview

- entry into force **August 1st 2024** , fully applicable **August 1st 2026** + **exceptions**, HOWEVER:
- **EU Digital Omnibus on AI** (proposed in November 2025, provisional agreement in May 2026)
  - **Simplifying** the digital legal framework (AI Act, GDPR, Data Act etc.), technical standards and support tools in place before the enforcement → legal certainty
  - **Extension of enforcement deadlines** for high-risk AI systems → stand-alone: **December 2027**, embedded: **August 2028**
  - Significant changes: **physical / industrial AI** (inc. machines equipped with high-risk AI, e.g. autonomous machines, robots) → no overlapping rules for machinery product safety (only compliance with sectoral safety rules) & narrowing down the definition of "safety component" → relevance for **food safety, particularly in agriculture!**
  - Other changes: prohibition of "nudification" AI systems, delaying application of watermarking obligations on AI-generated content, possibility of personal data processing where strictly necessary to detect and correct biases, extending SME exemptions from certain rules etc.

holi food

AI Act – an Overview

It applies to…..'AI system(s)'

- a machine-based system
- designed to operate with varying levels of autonomy
- may exibit adaptiveness after deployment (self-learning capabilities, while in use)
- for explicit or implicit objectives infers, from received input, how to
- generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments

It does NOT apply to….

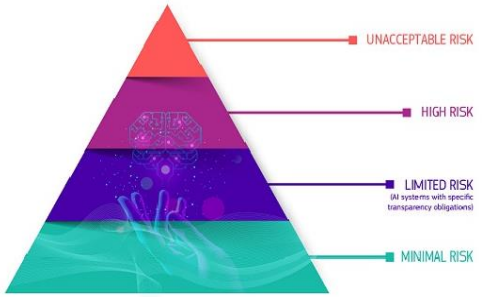
- sole purpose of scientific research and development, prior to their being placed on the market or put into service
- purely personal non-professional activity
- free and open-source licences, unless placed on the market or put into service as high-risk AI systems

holi food

AI Act – an Overview

1. **Unacceptable risk:** clear threat to the safety, livelihoods and rights → prohibited
   - harmful AI-based manipulation and deception, social scoring, emotion recognition in workplaces and education institutions, biometric categorisation etc.

2. **High-risk**: can pose serious risks to health, safety or fundamental rights → mandatory obligations
   - 1. AI system used as a (**safety component** of a) product **regulated by one of the listed EU harmonisaion regulations** (Annex I) + required third-party conformity assessment
     - Safety component: a safety function or its failure/malfunction endangers health and safety of persons and property
       - Digital omnibus narrowing down: if its intended purpose is to prevent/mitigate risks to the health and safety of persons/property
   - 2. AI system used in the **"sensitive" field** (listed in Annex III)
     - e.g. biometric identification, management and operation of critical infrastructure, education, law enforcement, migration etc.



Source: European Commission, AI Act, A risk-based approach

holi food

AI Act – an Overview

Providers of **high-risk AI systems** are responsible for compliance regarding:

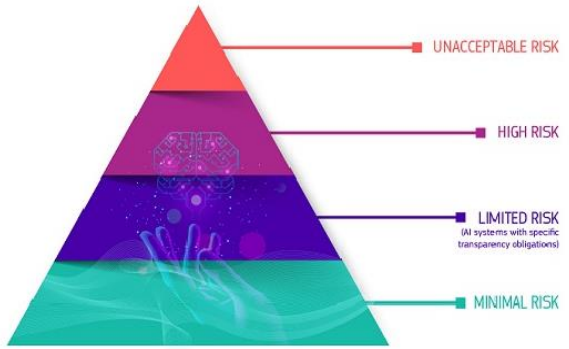
- adequate risk assessment and mitigation systems
- adequate, representative, high-quality of the datasets feeding the system
- detailed documentation for authorities to assess its compliance & clear and adequate information to the deployer
- appropriate human oversight measures

3. **Limited-risk**: transparency obligations → e.g. informing users, labeling AI-generated content

- AI systems Interacting directly with natural persons (e.g. Chatbots)

4. **Minimal risk**: no obligations, voluntary codes of conduct

- majority of AI systems e.g. AI-enabled video games or spam filters



Source: European Commission, AI Act, A risk-based approach

AI Act and Food Safety

Unaccepted risk (prohibited) → Limited relevance in food safety, indirectly e.g. manipulative/deceptive AI in nutrition apps (exploiting cognitive decline or emotional vulnerability to drive subscription)

High-risk (strict obligations)

- As a safety component / product under sectoral EU regulation listed in the AI Act
  - Core EU regulations on food safety not included (e.g. hygiene of foodstuffs, food of animal origin, microbiological criteria)
  - Regulation on the approval and market surveillance of agricultural and forestry vehicles
    - e.g. tractors using AI systems, such as algorithms to prevent harm to bystanders
  - Machinery Regulation
    - E.g. other machinery and equipment using AI to automatically detect contamination → DO: exempted from applicability when overlap exist
  - Relevance through overlap with other sectors, e.g. Medical Device Regulation (nutrition decision support, dietary systems), Vehicle Safety Regulation (refrigerated transport, food logistics)
- Used in the "sensitive" field (Annex III) → Food safety not explicitly listed

holi food

Conclusion

- Research exemption under the AI Act supports development/testing of AI in food safety contexts
- Prohibited AI: generally unlikely in food safety; limited to indirect cases (e.g. manipulation, deception)
- High-risk AI: possible when AI is a safety component in agrifood or similar vehicles → mandatory compliance obligations, if not, only transparency obligations or voluntary codes of conduct apply, together with obligations from sectoral legislation (e.g. Machinery Regulation)
- Broader regulatory landscape still applies beyond the AI Act:
  - Ethical AI frameworks (trustworthy AI guidelines
  - GDPR, Digital Services Act, Digital Markets Act, Data Governance Act
  - Product Liability Directive

Thank you!

Questions?

eva.korenjak.lalovic@univie.ac.at

universität wien
Department of Innovation and Digitalisation in Law

holi food

Funded by the European Union