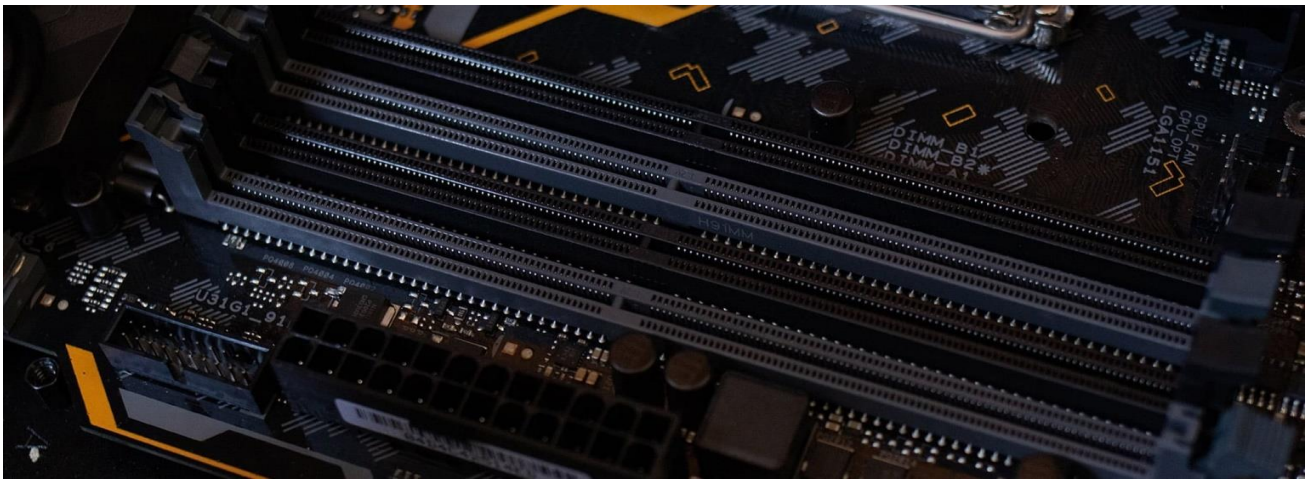

Top 10 Questions on the EU AI Act

1. What is the definition of an "AI system" under the EU AI Act, and what do the key elements of this definition signify?

The Act defines an "AI system" as *"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"*. The key aspects of this definition are: a) It must be a machine-based system, meaning running on machines, b) It must function with some degree of autonomy, operating independently of human intervention to a certain extent (although the precise level of autonomy required is not explicitly defined), c) It should have adaptiveness, or self-learning abilities, enabling it to evolve while in use (though this is optional, as the Act states it "may" exhibit this), and d) It infers information from input data, which can include text, speech, images, etc. The system then uses this input data along with set instructions or parameters to generate outputs like predictions (e.g., if X happens, Y might follow), content (such as images, graphs, text), recommendations, or decisions. The recitals clarify that this definition does not include simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations. The definition and its practical application are expected to become clearer through Commission delegated acts and guidelines.

2. Who is subject to the AI Act?

The AI Act applies only to areas within EU law and provides exemptions such as for systems used exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities, as well as for scientific research and development purposes. Here are the key points regarding its applicability:

a) Providers of AI Systems: The Act applies to any natural or legal person, public authority, agency, or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service within the EU, under its own name or trademark, whether for payment or free of charge.

b) Deployers/users of AI Systems: The Act applies to any person that has its place of establishment or is located within the EU and uses an AI system under its authority, except for this using AI

systems in the course of a purely personal non-professional activity.

c) Importers and Distributors: Those importing (person established in the EU that places on EU market and AI system that bears the name or trade mark of a non-EU person) or distributing (person other than the provider or importer that makes an AI system available on the EU market) AI systems within the EU are also subject to the Act.

d) Product manufacturers: Those placing on the market or putting into service an AI system together with their product and under their own name or trademark are subject to the Act.

e) Providers and Deployers outside the EU: The Act also applies to providers and deployers located outside the EU if the output produced by the AI system is used in the EU. This extraterritorial scope is designed to ensure that all AI systems impacting EU citizens are regulated, regardless of where the provider or deployer is based.

f) Authorised representatives of providers, which are not established in the Union: Any natural or legal person located or established in the EU who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by the Act.

g) Affected persons that are located in the EU.

3. How should non-EU-based organizations navigate the AI Act, and do they need to worry about its implications?

Non-EU organizations may be subject to the EU AI Act and should start by determining if they provide, import, or distribute AI systems in the EU, or if their AI systems produce outputs used in the EU. They must identify whether their AI systems fall under any regulated risk categories and clarify their roles (provider, importer, distributor, or deployer) to understand the regulatory requirements.

The AI Act applies to non-EU organizations if they place AI systems on the EU market or if the output of their AI systems is used in the EU. This means a non-EU provider developing AI systems for EU clients will be subject to the Act. Additionally, if an AI system's output is used within the EU, the non-EU organization must comply with the Act to prevent EU organizations from circumventing regulations by outsourcing AI activities. Providers of high-risk AI systems outside the EU must appoint an authorized representative within the EU.

4. How does the Act regulate AI systems?

Under the Act, AI systems are categorized based on risk levels, with each category subject to specific obligations and guidelines determined by a risk assessment methodology. The various AI systems have been classified into four categories based on their potential level of risk: (i) AI systems that are prohibited; (ii) AI systems with high risk; (iii) AI systems with limited risk (transparency risk); (iv) AI systems with minimal or no risk.

The prohibited AI systems include: (i) Manipulation of human behavior; (ii) Exploitation of vulnerabilities based on age, disability, or social and economic status; (iii) Social behavior-based classification of individuals or groups; (iv) Risk assessments for predicting criminal behavior solely based on profiling or personality traits; (v) Creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; (vi) The use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons; (vii) Biometric categorization systems inferring sensitive personal information such as race, political opinions, trade union membership, religious or philosophical beliefs,

sex life or sexual orientation; (viii) Real-time remote biometric identification systems (with exceptions).

High-risk AI systems are (i) those designated to serve as safety components of products or those considered products themselves, falling under Union harmonization legislation specified in Annex I and (ii) Additionally, AI systems listed in Annex III covering various sectors such as biometric systems, critical infrastructures, education and vocational training, employment, access to services, law enforcement, migration asylum and border control management, administration of justice, and democratic processes. High-risk AI systems are subject to stringent requirements, including documentation obligations, compliance measures ensuring bias monitoring, system robustness, accuracy, cybersecurity, data privacy standards, human oversight, and technical documentation. Furthermore, these systems (high-risk AI system listed in Annex III, with the exception of high-risk critical infrastructure AI systems) must be registered in the EU Database, and compliance for all high-risk AI systems will be indicated by affixing a CE marking denoting conformity.

Limited risk AI Systems: The AI Act imposes requirements on providers and sometimes deployers concerning transparency for AI systems that pose transparency risks. These include systems that interact directly with individuals or generate/manipulate text, video, audio, or images, such as chatbots, virtual assistants, and AI systems creating deep fakes.

Minimal risk or no risk AI Systems: Systems posing minimal risk to individuals (e.g., spam filters and recommender systems) will not be subject to additional obligations beyond existing legislation, such as the GDPR.

5. Have EU authorities released a simple tool (like a checklist or flowchart or some other type of document) to determine the AI system's risk level of your organization under the AI Act?

There's no official guide yet on how risky your AI system is under the EU AI Act.

However, the EU does offer some resources:

- EU Commission FAQs: This can help you understand the different risk categories.
- Independent legal assessment: It's recommended to have a lawyer assess your AI system against the Act's risk levels.
- The Act emphasizes training: People involved with your AI system should have the proper skills and knowledge.

Need help? If your organization lacks the expertise, consider getting appropriate counsel to navigate the risk assessment.

6. Will there be clarifying regulations and future guidelines related to the AI Act?

Yes, the AI Act includes provisions for the European Commission to issue implementing *(articles 41, 56, 57, 58, 60, 66, 92, 101)*, delegated acts *(articles 6, 7, 11, 43, 47, 51, 52, 53, 97)* and guidelines (96) to resolve remaining uncertainties. These acts could modify or introduce exemptions for high-risk AI systems, adjust the high-risk use cases listed in Annex III, and establish protocols for post-market surveillance of AI systems. Additionally, updates to the GPAI model's systemic risk threshold will be addressed through these acts. Guidance is also expected from the AI Board and national competent authorities. Forthcoming legislation and guidelines beyond the Act may include delegated acts defining AI systems, exemptions for high-risk AI systems, and rules for GPAI models, along with implementing acts for GPAI code approvals and generative AI watermarking. The Commission may also offer specific guidance on areas such as determining high-risk AI systems, applying AI system definitions, provider obligations for high-risk AI systems, and implementing transparency requirements for AI systems posing transparency risks. The AI Office and

national regulators are likely to contribute further codes of practice and guidance. In summary, ongoing developments are anticipated in this evolving regulatory landscape.

7. What is the transitional period under the AI Act?

The AI Act enters into force on the 20th day after its publication in the Official Journal. It shall apply from 2 August 2026.

It will be implemented gradually:

- Chapters I and II shall apply from 2 February 2025;
- Chapter III Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 shall apply from 2 August 2025, with the exception of Article 101;
- Article 6(1) and the corresponding obligations in the AI Act shall apply from 2 August 2027.

Organizations should ensure compliance with these timelines to avoid penalties under the AI Act.

8. What some examples of high-risk use cases are as defined in Annex III?

- Remote biometric Identification systems (this does not encompass AI systems designed for biometric verification whose sole purpose is to authenticate the identity of an individual), biometric categorization systems (AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics) and AI systems intended to be used for emotion recognition.
- Critical Infrastructure Management: Systems used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.
- Education and Vocational Training: AI used to determine access to education, assess students' performance, evaluate learning outcomes and steer the learning process as well as monitoring and detecting of cheating.
- Employment, Workers Management, and Access to Self-Employment: AI systems used for recruitment, task allocation, and monitoring of employees, e.g. to place targeted job advertisements, analyse and filter job applications, and to evaluate candidates.
- Access to essential private and public services and benefits (e.g. healthcare): Systems determining access to financial services, housing and social services; creditworthiness evaluation of natural persons; risk assessment and pricing in relation to life and health insurance; evaluation and classification of emergency calls.
- Law Enforcement: AI used for predictive policing, evidence analysis, and other law enforcement activities.
- Migration, Asylum, and Border Control Management: Systems used to assist competent public authorities for the examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, systems used in immigration and border control processes for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents.

- Administration of Justice and Democratic Processes: AI used in judicial systems and electoral processes.

9. What are the tasks of the European AI office?

- The European AI Office is responsible for supporting the AI Act and enforcing general-purpose AI rules by ensuring consistent application across EU Member States through advisory bodies and information exchange, developing tools and benchmarks to assess and classify AI models with systemic risks, collaborating with AI developers to create state-of-the-art codes of practice, investigating rule violations, and preparing guidelines for effective implementation and compliance.

- It also strengthens the development and use of trustworthy AI by promoting policies for societal and economic benefits, providing best practices, facilitating access to AI sandboxes, fostering innovation, and enhancing AI literacy.

- Additionally, the Office fosters international cooperation by advocating for the EU's trustworthy AI approach, supporting global AI governance, and aiding in the development of international agreements. Continuous monitoring of the AI ecosystem, technological advancements, market trends, and systemic risks informs its actions.

- The Office collaborates with various institutions, experts, and stakeholders, including the European Artificial Intelligence Board, the European Centre for Algorithmic Transparency, and an advisory forum of diverse stakeholders. It partners with experts and organizations to share best practices, oversees the AI Pact to engage businesses with the Commission and stakeholders, supports the European AI Alliance for open policy dialogue, and maps initiatives to promote trustworthy AI within the EU.

European AI Office | Shaping Europe's digital future (europa.eu)

10. What are the potential penalties for breaches of the AI Act?

When AI systems are marketed or utilized without meeting the AI Act's requirements, Member States must impose effective, proportionate, and dissuasive penalties, including administrative fines, and report these to the Commission.

The AI Act specifies penalty thresholds *(article 99)*:

- Up to €35 million or 7% of the total worldwide annual turnover of the preceding financial year (whichever is higher) for non-compliance with the prohibition of the AI practices.

- Up to €15 million or 3% of the total worldwide annual turnover of the preceding financial year for non-compliance with any of the following provisions related to operators or notified bodies, other than those laid down in Articles 5 (prohibited AI practices): a) obligations of providers pursuant to Article 16; b) obligations of authorised representatives pursuant to Article 22; c) obligations of importers pursuant to Article 23; d) obligations of distributors pursuant to Article 24; e) obligations of deployers pursuant to Article 26; f) requirements and obligations of notified bodies pursuant to Article 31, Article 33(1), (3) and (4) or Article 34; g) transparency obligations for providers and deployers pursuant to Article 50.

- Up to €7.5 million or 1% of the total worldwide annual turnover of the preceding financial year for the supply of incorrect, incomplete or misleading information to notified bodies or

national competent authorities in reply to a request.

In the case of SMEs, including start-ups, the applicable threshold is the lower of the two amounts, whereas for other companies, it is the higher amount.

Authors:

TMT & IT
M&A
Arbitration & DR
Employment & Pensions
Corporate
Chara Daouti
Partner
C.Daouti@lambadarioslaw.gr

TMT & IP

Virna Angelopoulou
Associate
V.Angelopoulou@lambadarioslaw.gr