

How LLM Capabilities Trigger AI Act Obligations

The better the question. The better the answer. The better the world works.

Shape the future with confidence

EY Law Technology - Agenda



Oktawia Sepioł

Project Manager

1 Part I

Identification of AI Systems

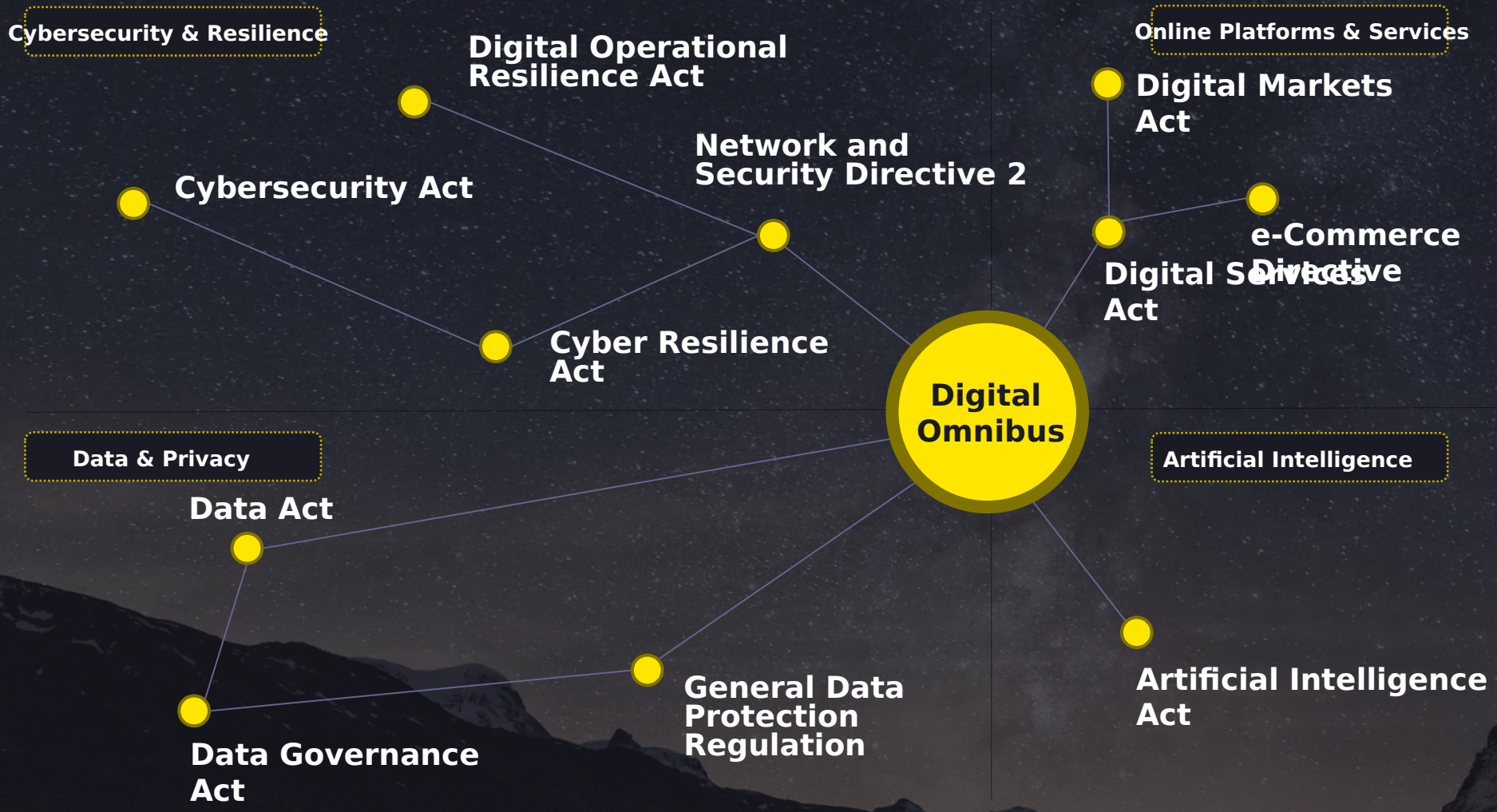
2 Part II

Classification of AI Systems

3 Part III

Legal Obligations Regarding High-Risk Systems

EU regulatory tsunami in the digital field is real

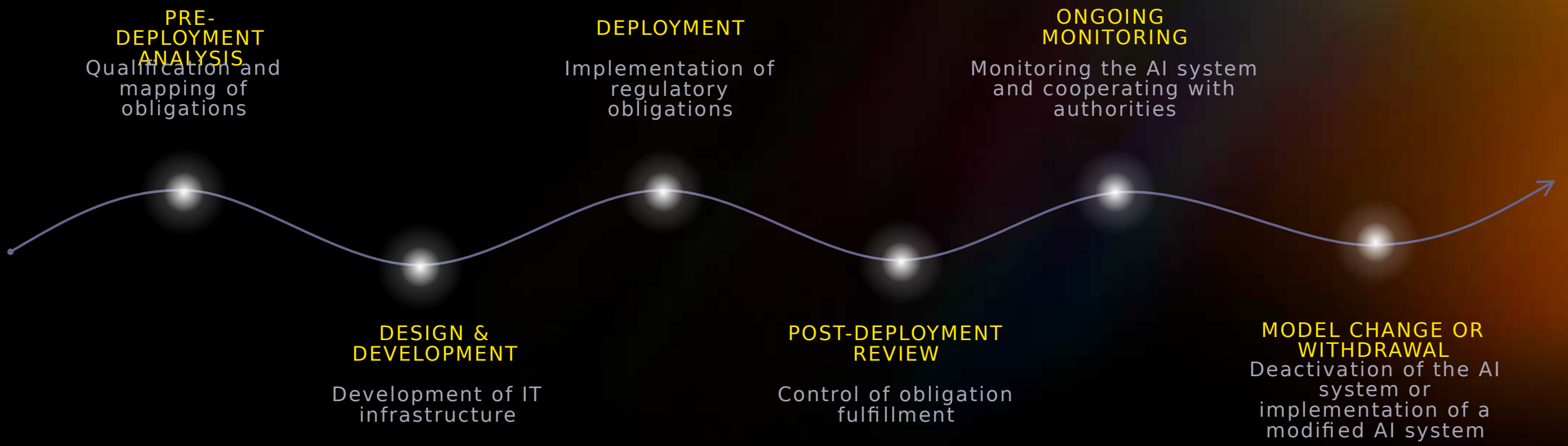


Companies across Europe are increasingly struggling to navigate a rapidly expanding regulatory landscape.

Regulatory tsunami is reshaping how organizations plan, invest, and innovate in digital technologies.

77% of firms report that regulatory complexity negatively affects their operations, with technology-related areas, emerging as some of the most heavily burdened domains.

Lifecycle of an AI System



AI Act – Actual Scope of Obligations

Process of Determining the Scope of Limitations and Obligations for a Specific System:

Qualification as an AI System

+

Assessment of the risk level

+

Defining the role of the entity using the system

+

Identification of regulatory obligations

+

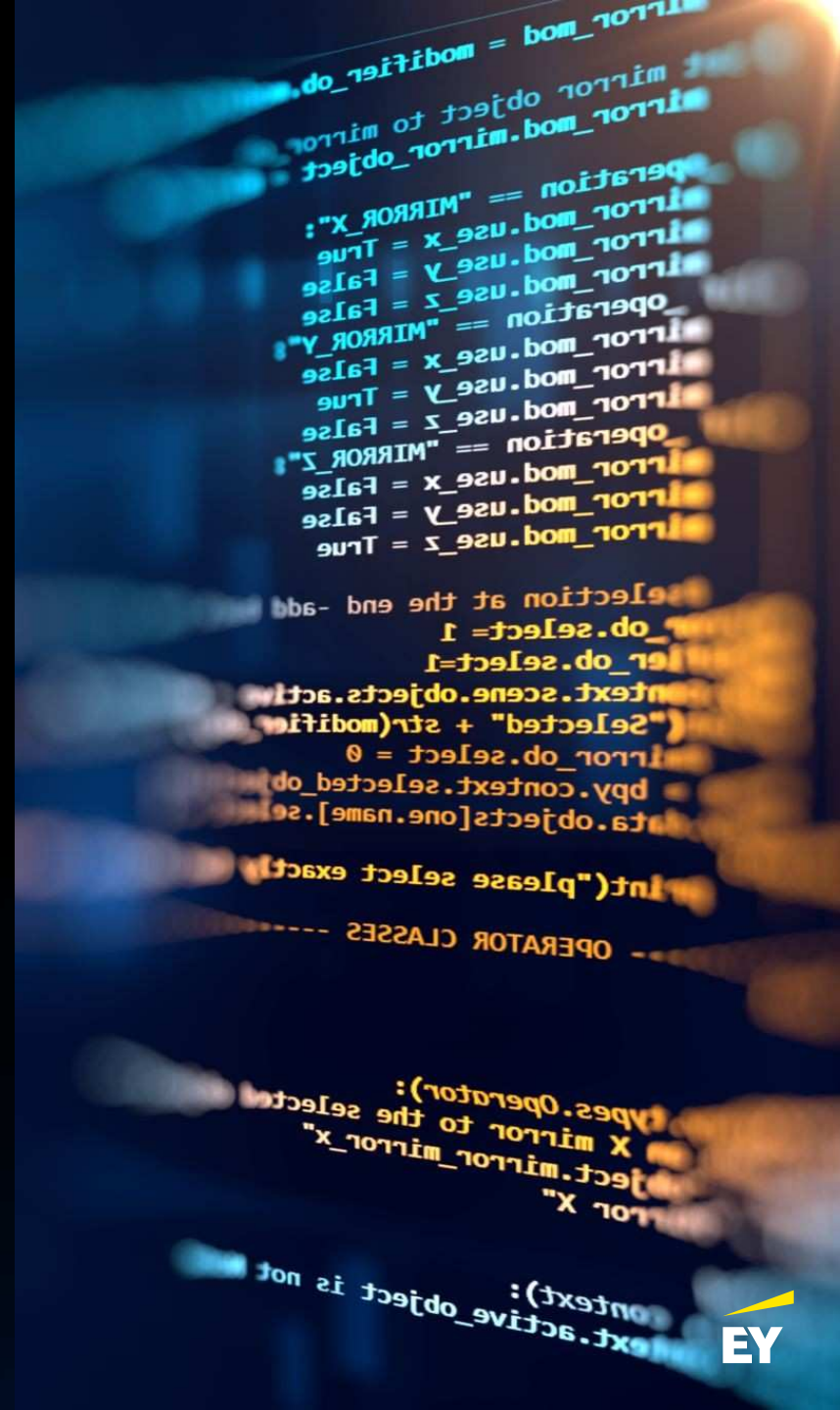
Consideration of Regulations Beyond the AI Act

Definition of an AI System

According to Article 3(1) of the AI Act, "AI system" means:

“

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



Classification of a System as an AI System

Key qualification criteria – Article 3 point 1) AI Act (+ explanations in Recital 12):

- **MACHINE-BASED** – „(…) The term ‘machine-based’ refers to the fact that AI systems run on machines.(…)”

  - **Is the system an IT system?**

    This applies regardless of the underlying technology, including cloud-based solutions.

  - **Are the system’s functions performed by or within machines or devices?**

    For example, through IT infrastructure, robots, or other types of machinery.

In most cases, the operation of typical IT systems will meet this condition.

Classification of a System as an AI System

Key qualification criteria – Article 3 point 1) AI Act (+ explanations in Recital 12):

- **AUTONOMY** – „(...) designed to operate with varying levels of autonomy, meaning that they have some degree of independence of actions from human involvement(...)"

  - **Is the system capable of generating outputs on its own?**

    This applies if the system can produce results as part of its functioning, without relying on a human at every step.

  - **Does the system perform at least part of its functions autonomously?**

    It doesn't matter if the human needs to start the system, enter a command, or ask a question. Partial autonomy is enough.

  - **Can the system generate some portion of the results without human intervention?**

    If the system can produce any part of the output on its own, this indicates autonomous operation.

Classification of a System as an AI System

Key qualification criteria – Article 3 point 1) AI Act (+ explanations in Recital 12):

- **(?) ADAPTIVENESS** – „(…) The adaptiveness that an AI system could exhibit after deployment, refers to self-learning capabilities, allowing the system to change while in use. (…)”

  - **Can the system, as a whole, independently make lasting changes to the way it operates after deployment?**

    This refers to situations where the system adjusts its own rules or behaviour over time, based on user interactions or the data it processes.

  - **Can the system improve or alter parts of its decision-making process without human intervention?**

    If the system refines or restructures any component of the model on its own, this also meets the adaptiveness criterion.

  - **Does the way the system operates change over time?**

    If the system’s functioning is not fixed but shifts based on experience, this is a sign of adaptiveness.

Classification of a System as an AI System

Key qualification criteria – Article 3 point 1) AI Act (+ explanations in Recital 12):

- **INPUT-BASED INTERFERENCE of how to generate outputs** – „(…) The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning or modelling. (…)”

  - **Does the system independently choose how to solve a task or achieve its goal?**

    This checks whether the system selects data or action paths on its own — in ways that are not fully predefined or predictable.

  - **Are the system’s internal operations fully predictable and fixed in advance?**

    This criterion is met if a human can fully explain and predict all the steps in the system’s operation.

  - **Does the system always produce the same, fully explainable output for the same input?**

    It is met, if the results can’t be predicted with complete certainty before running the system

  - **Does a human have the ability to reliably and predictably influence the**

Classification of a System as an AI System

Key qualification criteria – Article 3 point 1) AI Act (+ explanations in Recital 12):

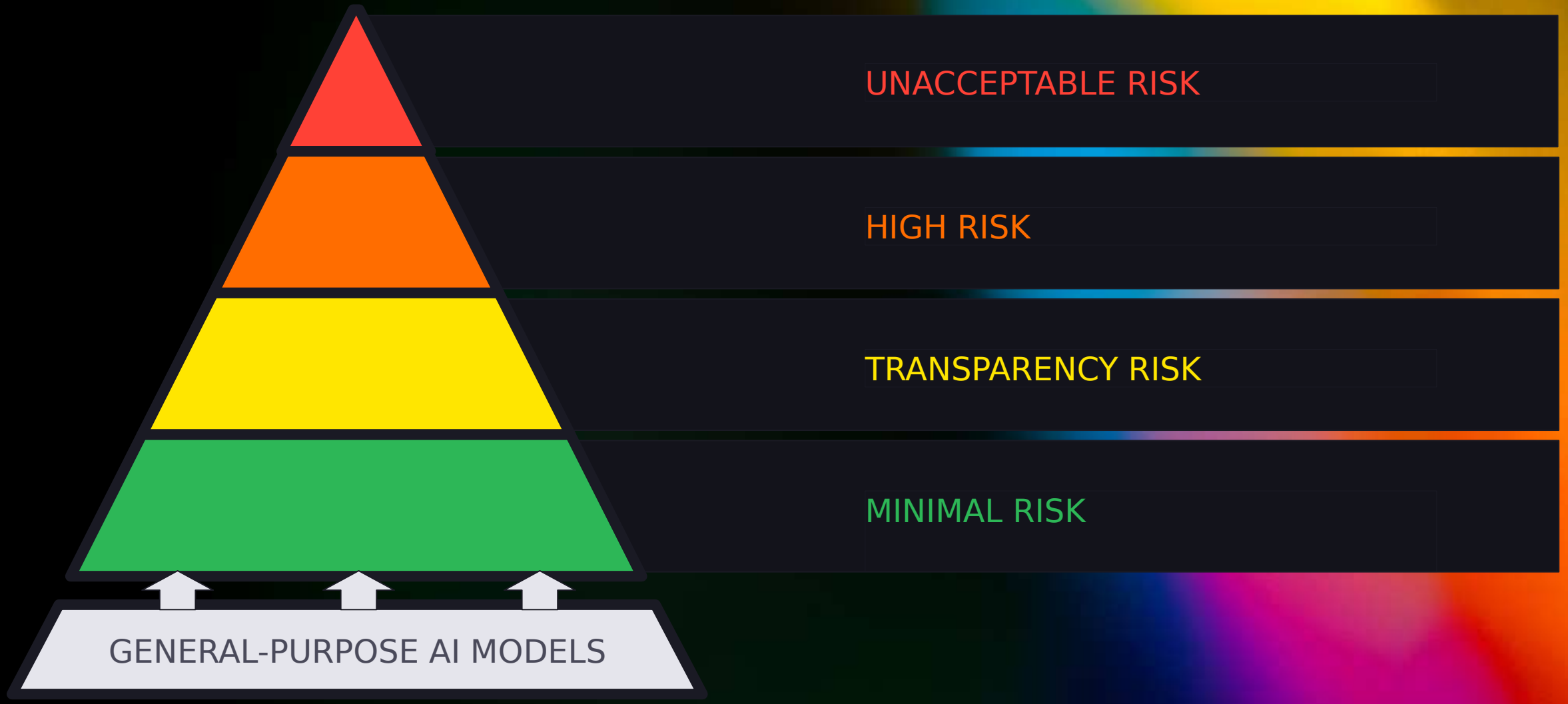
- **GENERATING RESULTS** – „(...) outputs generated by the AI system reflect different functions performed by AI systems and include predictions, content, recommendations or decisions.(…)”
- **IMPACT ON THE VIRTUAL OR PHYSICAL ENVIRONMENT** – „(…) For the purposes of this Regulation, environments should be understood to be the contexts in which the AI systems operate (...)”

  - **Do the system’s outputs have the potential to trigger or shape actions, decisions, content?**

  Any output that leads to a change in a digital or physical system meets this criterion.

In practice, most IT systems generate outputs that influence other systems, data, or processes — which means this criterion is usually fulfilled.

AI Act – Risk Principle



Qualification of AI Systems – Prohibited Practices

The classification of AI systems into the category of unacceptable risk under the AI Act includes systems that are considered particularly harmful and pose a threat to the safety, rights, and values of the EU. This category includes AI systems that:

- Use subliminal and manipulative techniques
- Assess the emotions of individuals
- Exploit the vulnerabilities of individuals
- Conduct risk assessments based on profiling individuals



- Categorize individuals based on biometric characteristics
- Implement social scoring systems
- Conduct biometric identification of individuals
- Are used for indiscriminate image capture

Prohibited Practices – Article 5 AI Act

Article 5 paragraph 1 letter a) of the AI Act:

The following AI practices shall be prohibited:

the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

subliminal techniques are prohibited if:

impact the behaviour of a person or impact ability to make an informed decision

+

casue taking an decision or likely to cause harm

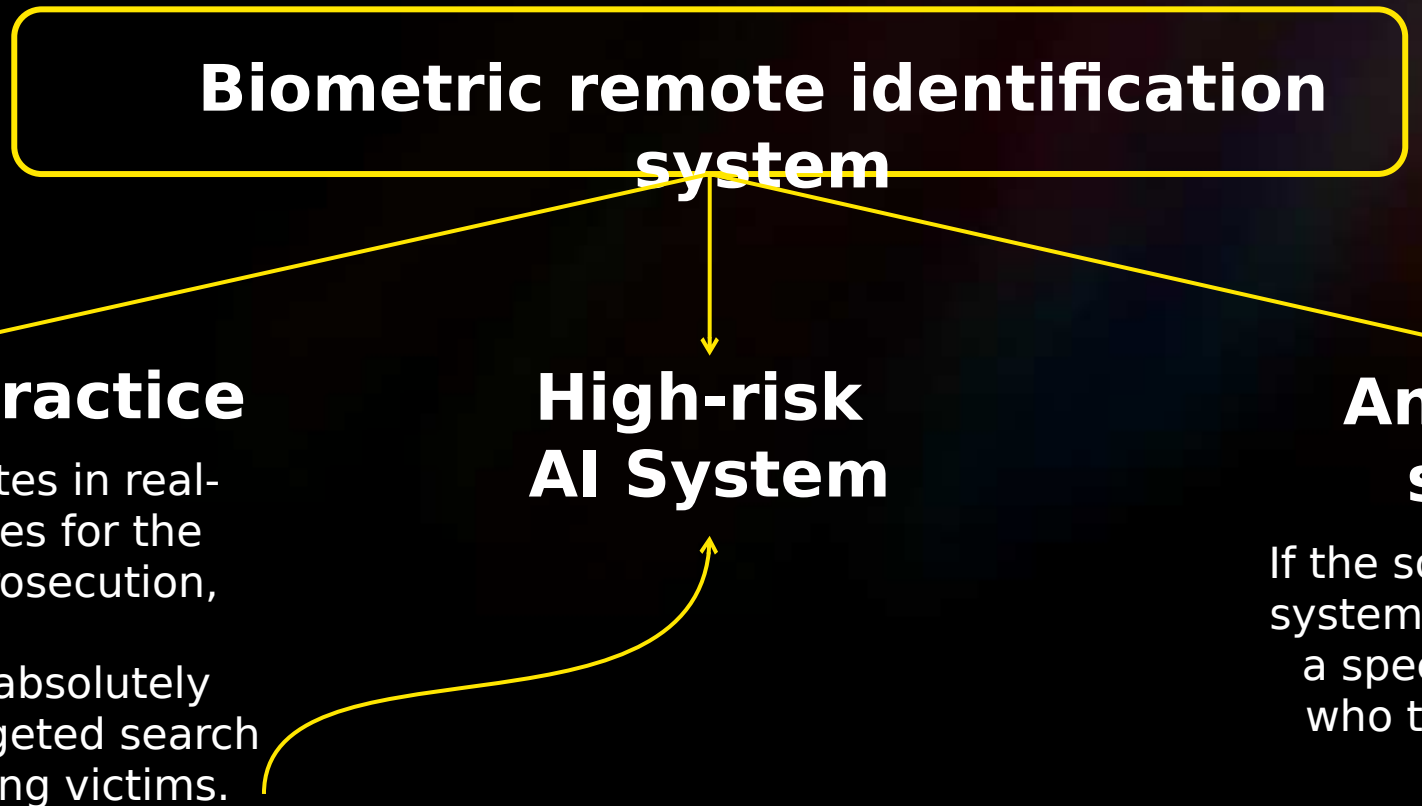
Qualification of AI Systems – High-risk Systems

- Risk classification based on the intended use of the AI system
- High risk AI systems:

Biometric systems	Employment
Critical infrastructure	Essential and public services
Education	Crime prosecution
Migration and border control	Justice system
Democracy	Product safety

Complicated Definitions

It is not possible to qualify an AI system solely based on its intended purpose or the method of operation used. The qualification of an AI system must take into account the full context of the system's operation.



Qualification of AI Systems – Systems Subject to Informational Obligations

- This is not a separate category of AI systems – high-risk AI systems may be subject to informational obligations.

Intended for direct interaction with individuals

Emotion recognition

Generating synthetic content

Generating content published for the purpose of informing the public

Biometric categorization

Deepfake and content manipulation

Qualification of AI Systems – other AI Systems

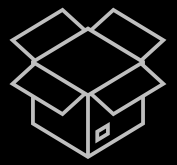
- **No specific regulation**
- No specific obligations – general obligations remain

Article 4 of the AI Act

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.

Entities Covered by the AI Act

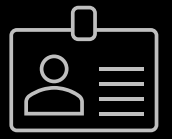
OPERATOR



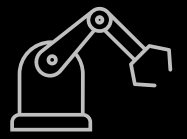
Provider



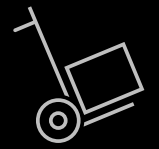
Deployer



Authorised representative

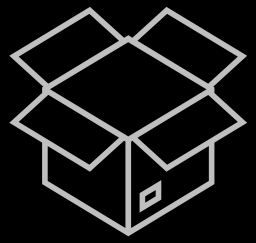


Product manufacturer



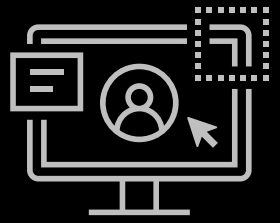
Importer or distributor

AI Act – Entities in the Value Chain



Provider

means a 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 under its own name or trademark, whether for payment or free of charge (Article 3 point 3 of the AI Act)



Deployer

means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity (Article 3 point 4 of the AI Act)

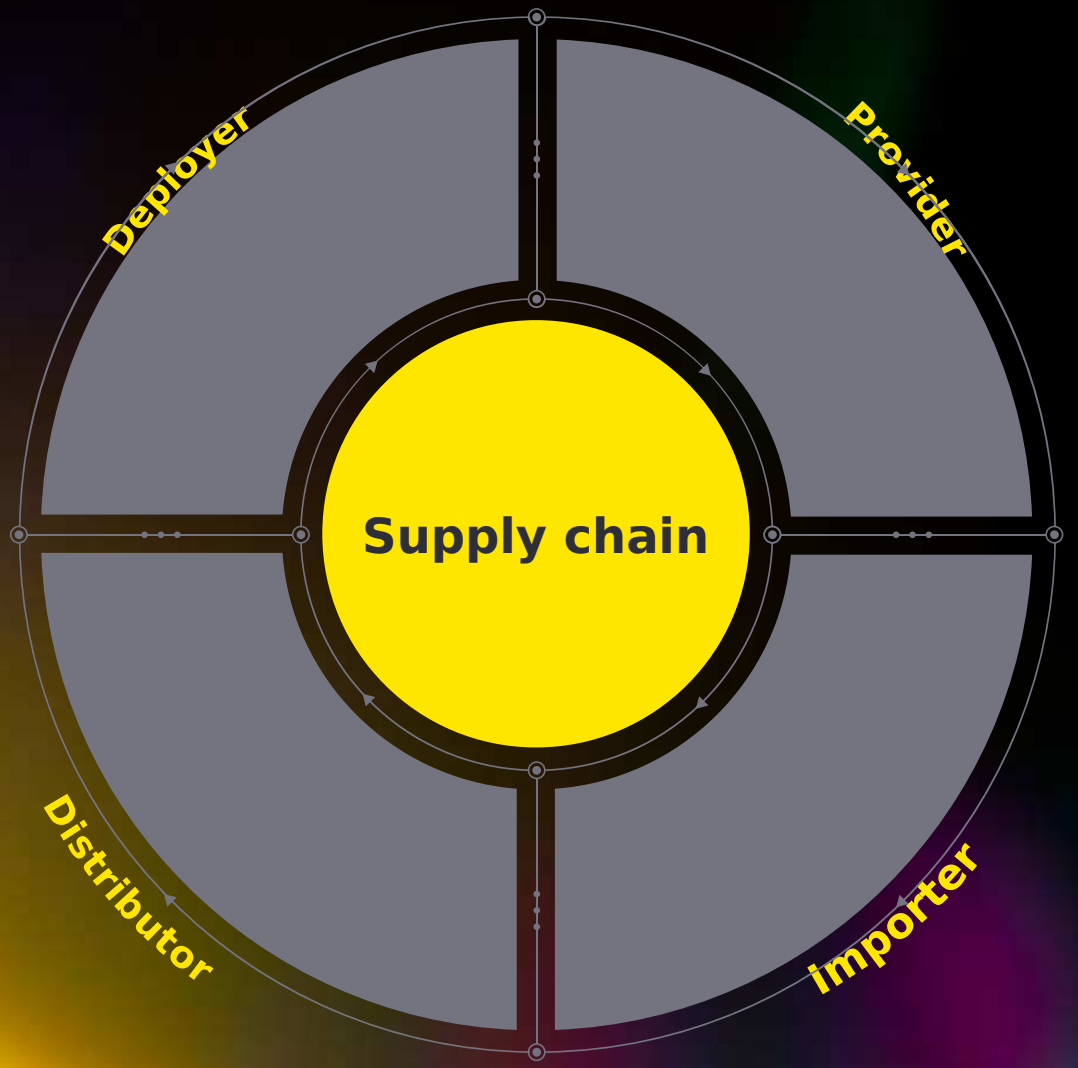
AI Act – Entities in the Value Chain

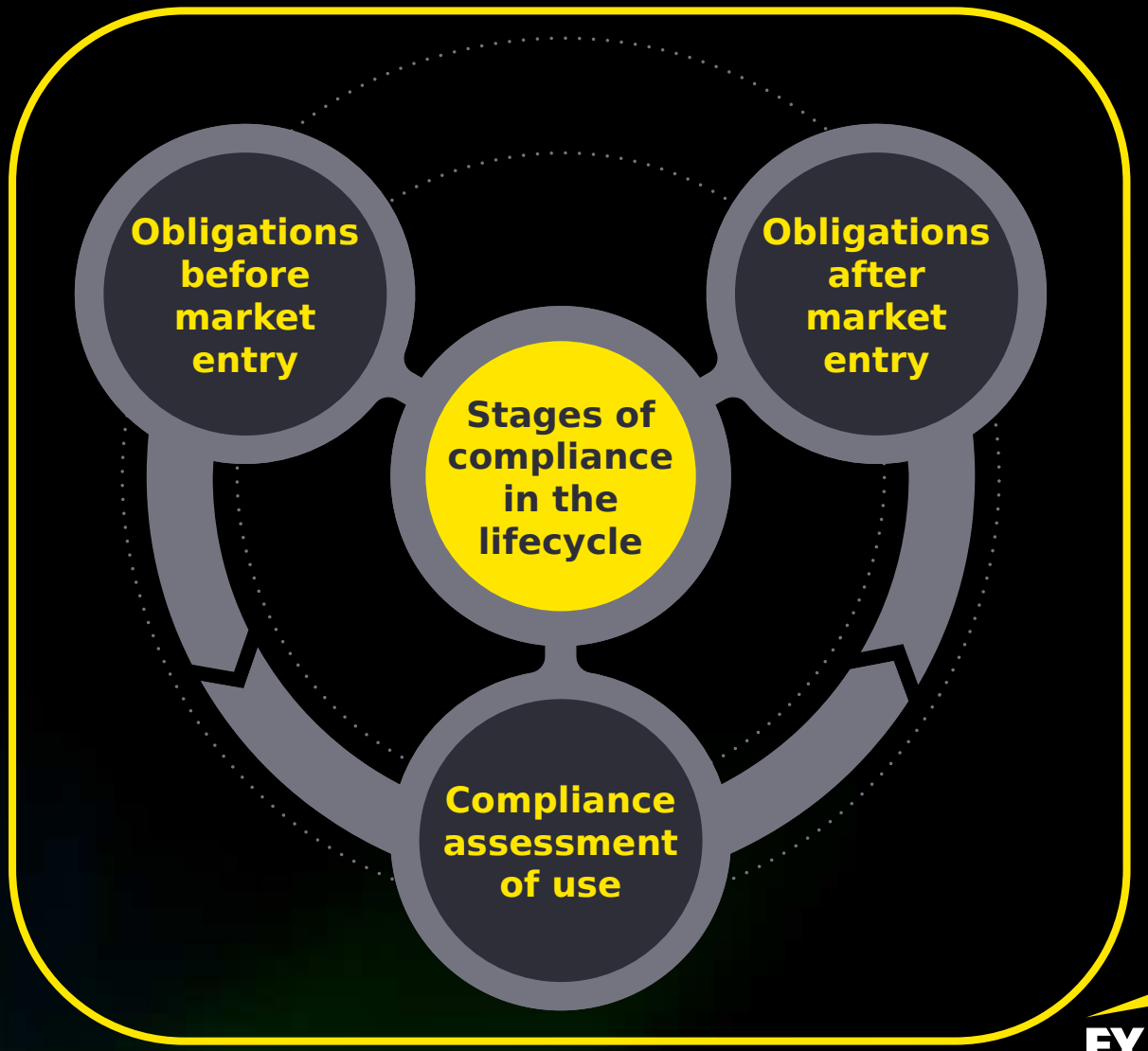
- **The main regulatory burden is placed on providers!**
- Limited obligations are also imposed on users (and other groups of entities).
- **NOTE! The AI Act introduces specific regulations that change the classification of entities!**

For example, Article 25 paragraph 1 of the AI Act: „**Any distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system** for the purposes of this Regulation and **shall be subject to the obligations of the provider under Article 16**, in any of the following circumstances:

- **they put their name or trademark on a high-risk AI system already placed on the market or put into service,** without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated;
- **they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system pursuant to Article 6;**
- **they modify the intended purpose of an AI system, including a general-purpose AI system,** which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system in accordance with Article 6.

Obligations at Every Stage of the Value Chain and Lifecycle of AI Systems



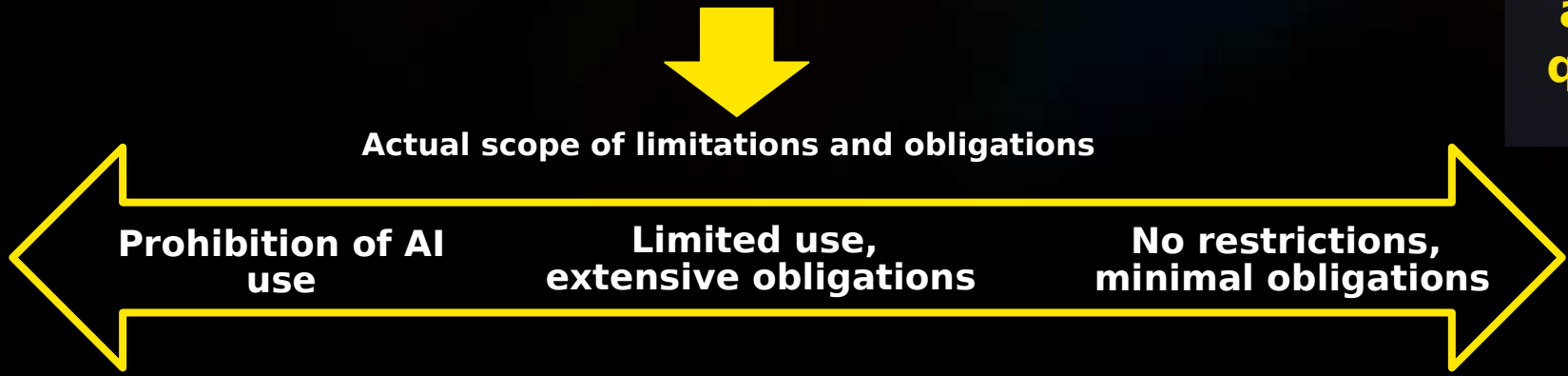


AI Act – Basic Analysis

To determine whether and how we should implement new regulations, we must answer the following questions:

1. What systems are we using or planning to implement?
2. Is the system an artificial intelligence system?
3. Is the system a general-purpose model?
4. Will the results of the system's work be used in the EU?
5. What is the organization's role in the lifecycle of the system?
6. To which category (based on the level of risk) should the examined system be classified?
7. What obligations apply to us?

The earlier in the process of developing or implementing an artificial intelligence system we answer these questions, the better.



Obligations of Providers Before Market Entry

Classification of the risk level of the AI system			
If prohibited	**If high risk**	**If limited risk**	**If minimal risk**
Prohibition of implementation of the AI system Or Necessity to deactivate the AI system	Risk management system and testing of systems	Transparency and informing	None (option to use voluntary codes of conduct)
	Quality management system and data sets		
	Technical documentation in accordance with Annex IV		
	Accuracy, robustness, and cybersecurity		
	Automatic event logging		
	User manual and human oversight measures		
	Compliance assessment and declaration of conformity		
	Labeling of the AI system		
	Registration obligations		

Obligations of Providers After Market Entry

Classification of the risk level of the AI system			
If prohibited	**If high risk**	**If limited risk**	**If minimal risk**
Prohibition of implementation of the AI system Or Necessity to deactivate the AI system	Event log storage	Transparency and informing	None (option to use voluntary codes of conduct)
	Updating and storing documentation		
	Ensuring availability requirements		
	Quality management system and monitoring		
	Incident reporting		
	System compliance control		
	Remedial actions		
	Cooperation with authorities and demonstration of compliance		

Obligations of the Deployers

Classification of the risk level of the AI system			
If prohibited	**If high risk**	**If limited risk**	**If minimal risk**
Prohibition of implementation of the AI system Or Necessity to deactivate the AI system	Using and monitoring the system in accordance with the instructions	Transparency and informing	None (option to use voluntary codes of conduct)
	Ensuring the quality of input data		
	Informing the provider and cooperating with authorities		
	Storing event logs		
	Competent human oversight		
	Compliance with registration requirements		
	Assessment of impacts on fundamental rights		
	Informing users		



Oktawia Sepioł

Project Manager

oktawia.sepiol@pl.ey.com
+48 518 814 649

Thank you for your attention, and I invite you to get in touch!

Q&A

