

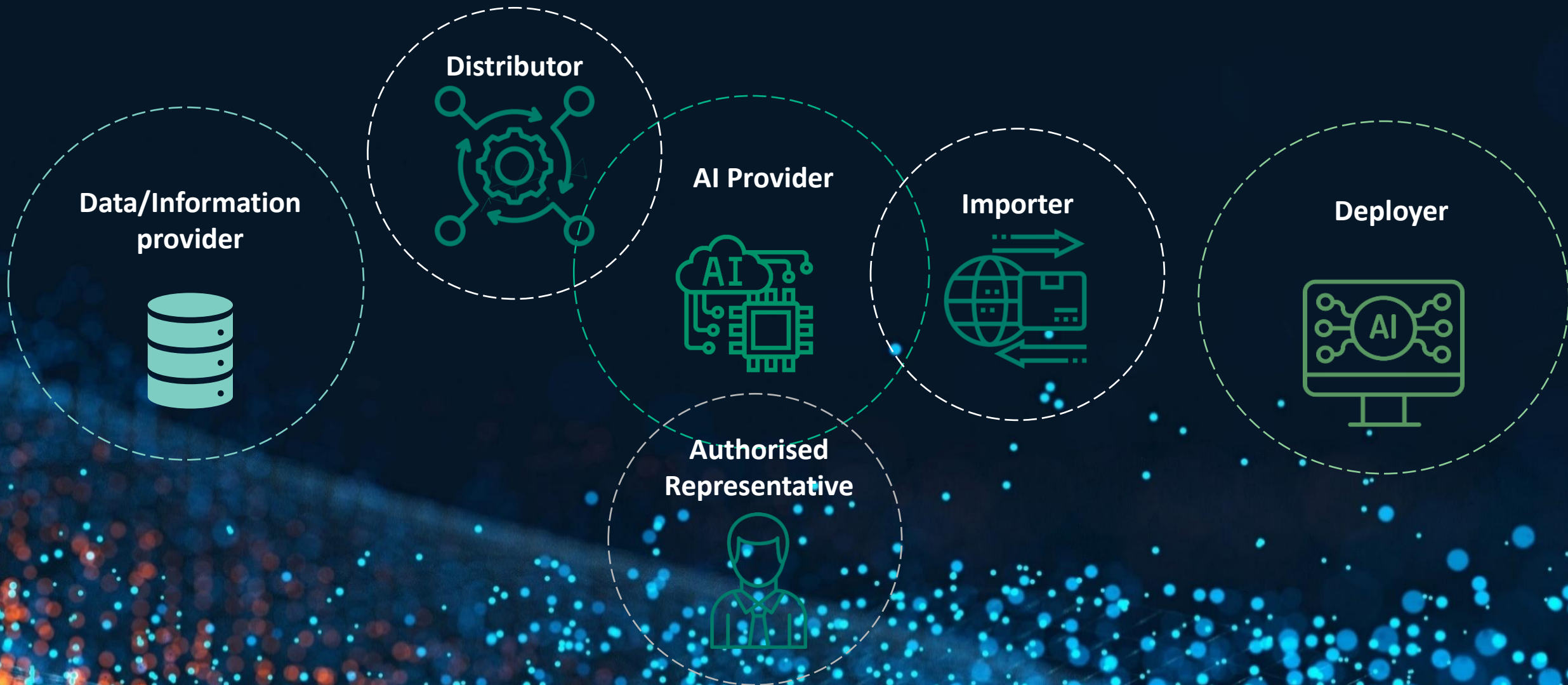


**AI Act**

# “AI Lifecycle” (simplified)



# The AI Ecosystem (simplified)





**Zoom In**

AI Act

# AI Act



## BROAD SCOPE OF APPLICATION

Obligations for most **stakeholders** in the **AI value chain** and **extraterritorial** scope of application covering AI systems outside the EU (sale , offer, put into service)



## RISK-BASED APPROACH

Prohibited risk » High-risk » Limited / Specific Risk (including a tiered-approach for GPAI & GenAI) » Minimal Risk



## NEW OBLIGATIONS

**Providers** and **deployers** of high-risk systems are particularly impacted by the new rules and are subject to obligations such as risk assessment, transparency, human supervision, training, data governance for training and testing datasets



## NEW AUTHORITIES

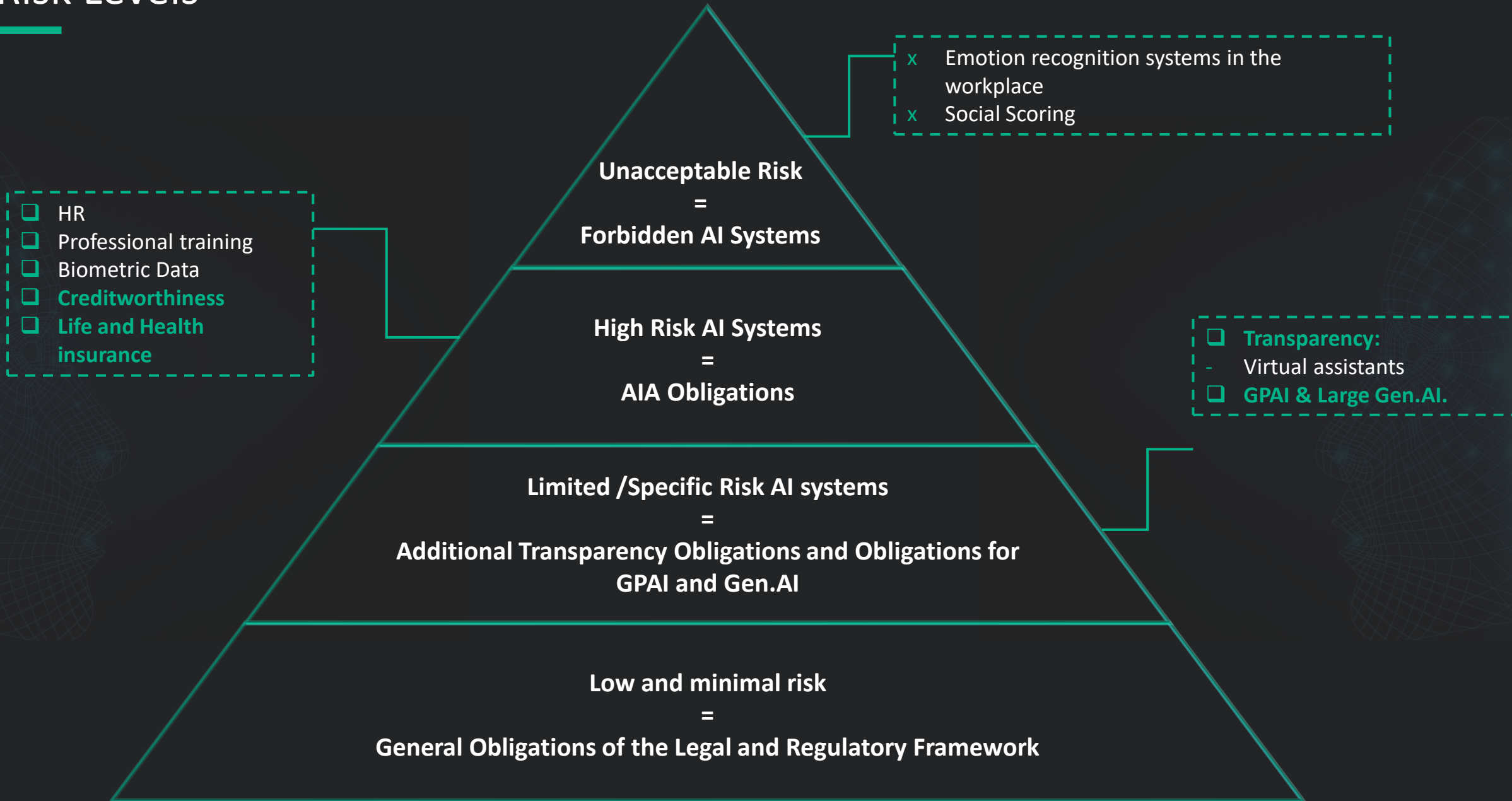
Every **MS** should appoint a new national authority responsible for supervising the application and implementation of the of the Regulation. New EU authorities are also created: **EU AI Office & EU AI Board (the Scientific Panel of independent experts )**



## FINES

**35 000 000 EUR** or until **7%** of the total annual worldwide turnover for the previous financial year, whichever is the higher.

# Risk Levels



# What types of systems are covered by the various risk levels?

## Prohibited AI-systems

- i) AI systems that deploy **subliminal techniques** beyond a person's consciousness to distort the person's behaviour in a harmful manner
- ii) AI systems targeting **vulnerabilities** of a specific group in a harmful manner
- iii) Systems that classify people on the basis of **sensitive data**, e.g. ideology, religion, sexual orientation, etc.
- iv) **Social scoring**
- v) Use of **'real-time' remote biometric identification and scrapping facial images for building databases** in publicly accessible spaces for the purpose of law enforcement except under one of the exceptions provided for in the Regulation
- vi) **Untargeted face scrapping** from the Internet or CCTV footage
- vii) **Emotion recognition systems** in the **workplace** and in **education**

## High-Risk AI Systems



Safety components in **vehicles**



Safety components in **medical devices**



(i) Remote **biometric identification**; (ii) Biometric **categorisation** of natural persons based on sensitive characteristics and (iii) (permitted) **Emotion recognition**



**Management and operation of critical infrastructures** (e.g. water, gas, heating, electricity, internet)



**Education & professional training**



**Recruitment, employment, management of employees and access to self-employment**



Access to and use of essential public and private services: (i) **public services and benefits** (e.g. health, insurance, etc.); (ii) **creditworthiness or credit scoring**; (iii) **emergency systems, including patient triage in healthcare**; (iv) risk assessment and pricing systems in **life and health insurance**.



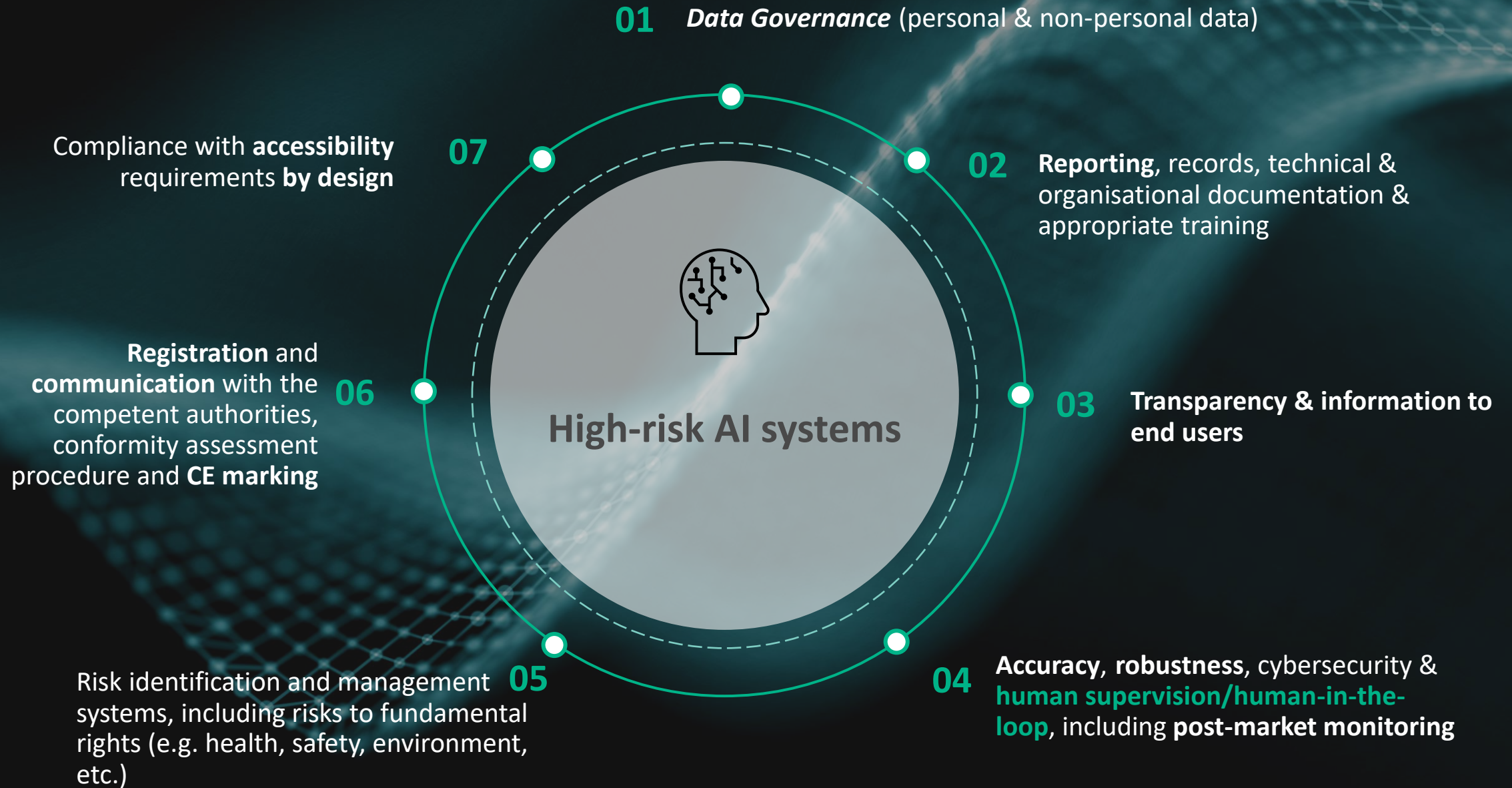
**Administration of justice and democratic processes**



Law enforcement, managing migration, asylum and border control

+ AI systems that present a significant risk of harming people's **health, safety or fundamental rights**.

# Obligations applicable to providers



# Obligations applicable to **Deployers**



**Technical and organisational measures**



Relevant automatic logs for 6 months



Relevant, adequate and sufficiently representative **input data**



Consult **workers' representatives** before implementing high-risk AI systems in the workplace



**Human supervision** and ensuring competence, qualifications, **training** and resources



Obligations of transparency and the right to explanation



Monitor, adjust and update **robustness** and **cybersecurity** measures



**DPIA & Fundamental Rights Impact Assessment ("FRIA")**



**Risk for provider to be considered provider**

# Obligations relating to Limited or Specific Risk AI Systems

## Transparency



**Providers of AI systems intended to interact with individuals**



**Providers of GPAI and Gen.AI systems**



**Deployers of permitted emotion recognition systems and biometric categorisation systems**



**Deployers of *deep fakes***

## *General-Purpose AI (“GPAI”) models and Large Generative AI Models*

- ❑ Tiered-approach: GPAIs with systemic risks, Large Gen. AI models used on a large scale, exception for open source Gen.AI systems
- ❑ Organisational policies and measures, **including risk assessment, technical documentation, data governance, EU representative**
- ❑ **Transparency obligations and obligation to publish a summary of the content used to train the model**

# Provisions relating to innovation



**Limiting unfair contractual terms imposed unilaterally on SMEs and startups**



Promoting the **participation of start-ups and SMEs in sandboxes**, simplification of quality management obligations and exceptions to **GPAI obligations**



**1 regulatory sandbox** per Member State or in collaboration with several Member States, under the supervision of national control authorities (the AI Office establishes the criteria for participation, the procedure and the participants' T&Cs) within 24 months of entry into force



Specific rules for **re-using data in the Sandbox = new basis for lawfulness under conditions ≠ further processing = GDPR and Data Act**



**Real-world testing** of AI systems, including high-risk systems, subject to authorisation and collaboration with supervisory authorities and under specific conditions, including the informed consent of the participant



Promoting AI **research and development** in support of beneficial outcomes for society and the environment at Member State level (**AI4Good**)



**AI**

Legal challenges and strategies

## Sector-specific obligations

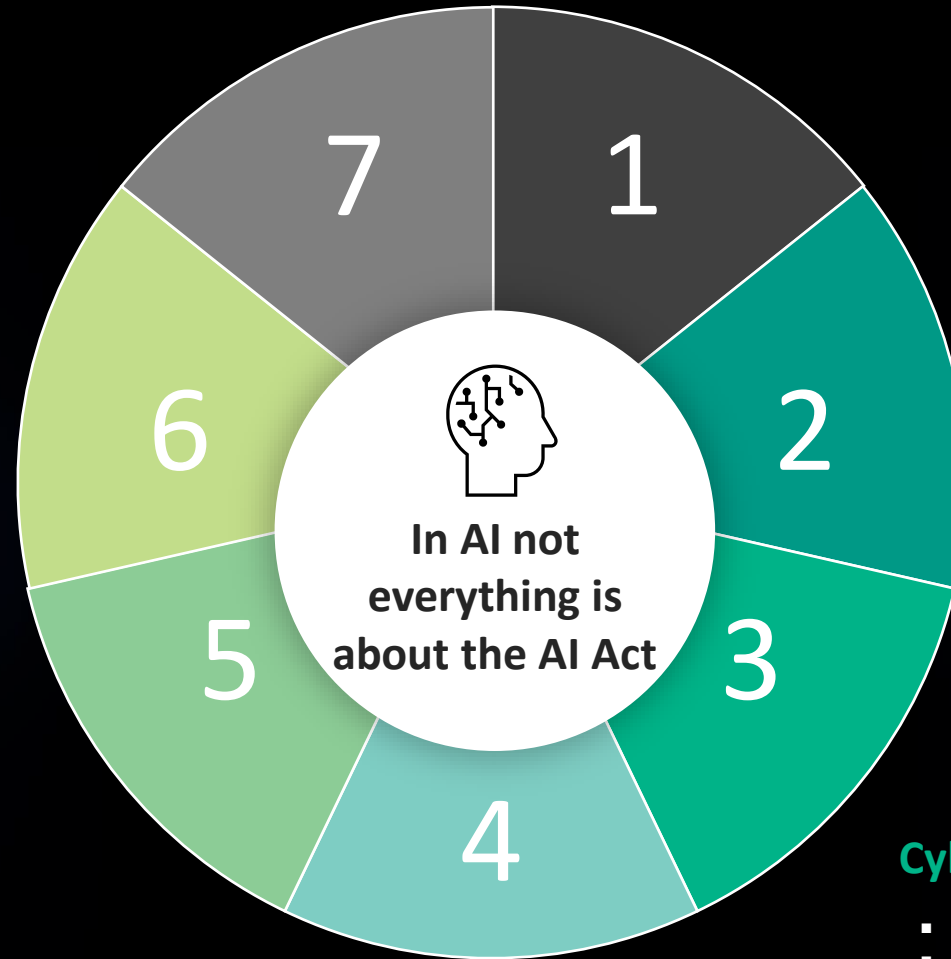
- Life sciences
- Banking and Finance
- Critical Infrastructure
- Digital Marketing
- HR

## Intellectual Property Rights

- IPR management of data and algorithm
- IPR management of AI outputs
- Confidentiality
- Trade secrets

## Product safety & consumer protection

- Product safety framework
- Contractual relations with stakeholders
- Instructions & Information
- Liability: system failures and violation of rules
- [PLD II \(approved\)](#) & [AI Civil Liability Directive](#)



## Fundamental Rights

- Biases & non-discrimination
- Information
- Health, safety, sustainability

## “AI-Specific Regulatory Framework”

- **AI Act Obligations**
- Sector-specific obligations for IA

## Data

- *Data Governance* (personal and non-personal data)
- **Personal data:** international data transfers & automated decision making
- Data accessibility & Data Quality
- *Data sharing* → **Data Act**
- “Biases” & errors
- **Contractual relations with stakeholders**

## Cybersecurity

- System failures
- Responsibility
- Insurance
- Sector-specific obligations

# What can companies do?

MAP AI USE CASES, THE AI ECOSYSTEM, AND AI TRAINING, TESTING AND FINE-TUNING DATASETS

01

CARRY OUT A LEGAL RISK IMPACT ASSESSMENT OF THE AI USE CASE TO IDENTIFY RISKS AND PRIORITISE MITIGATION MEASURES

02

UPDATE CURRENT INTERNAL POLICIES AND CONTRACTS IN LINE WITH THE LEGAL FRAMEWORK & INTERNAL AI STRATEGY

03

IDENTIFY A MULTIDISCIPLINARY TEAM DEDICATED TO AI AND PROVIDE TRAINING TO IDENTIFY BIASES AND ERRORS IN THE SYSTEM

04

PROVIDE CLEAR INFORMATION, INCLUDING OPT-OUT MECHANISMS

05

 VIEIRA DE ALMEIDA

[www.vda.pt](http://www.vda.pt)