

AI Compliance

Was bedeutet der
EU AI Act für mein
Unternehmen?

9. Oktober 2024



Your presenters today



Torsten Berge

Director | Audit & Assurance | AI & Algorithm Assurance

tberge@deloitte.de

+49 151 5807 2499

Deloitte GmbH Wpg



Jan Grüne

Director | Risk Advisory | Internal Audit

jgruene@deloitte.de

+49 171 8180 644

Deloitte GmbH Wpg

Strawberry counting r's in "Strawberry"



ChatGPT o1-preview >

How many Rs in a word straberry

Thought for 5 seconds ▾

The word "straberry" contains three "R"s. If you meant "strawberry," it has two "R"s.

You sure

Thought for 7 seconds ▾

Yes, I'm sure. The word "straberry" contains three "R"s:

1. The first "R" is the third letter.
2. The second and third "R"s are consecutive, appearing as the seventh and eighth letters.

If you meant "strawberry," that word contains two "R"s.

How many Rs in strawberry

Thought for 4 seconds ▾

The word "**strawberry**" contains two "R"s.

Wrong

Headlines on AI issues

OPENAI'S GPT IS A RECRUITER'S DREAM TOOL. TESTS SHOW THERE'S RACIAL BIAS

Recruiters are eager to use generative AI, but a Bloomberg experiment found bias against job candidates based on their names alone

FTC investigates OpenAI over data leak and ChatGPT's inaccuracy

The agency's demand for OpenAI's documents marks the company's greatest U.S. regulatory threat to date

Denied

The Secret Bias Hidden in Mortgage-Approval Algorithms

Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software

Apple's 'sexist' credit card investigated by US regulator

HEALTH AND HUMAN SERVICES

Nurses Worry About Lack of AI Rules in Hospitals

Time to act

OPENAI'S GPT IS A RECRUITER'S
DREAM TOOL. TESTS SHOW
THERE'S RACIAL BIAS

Recruiters are eager to use generative AI, but tests show racial bias against job candidates based on their names.

Denied

The Secret Service
Mortgage-App

FTC investigates OpenAI over data leak
and ChatGPT's inaccuracy

The agency's demand for OpenAI's documents marks the company's greatest U.S. regulatory threat to date.

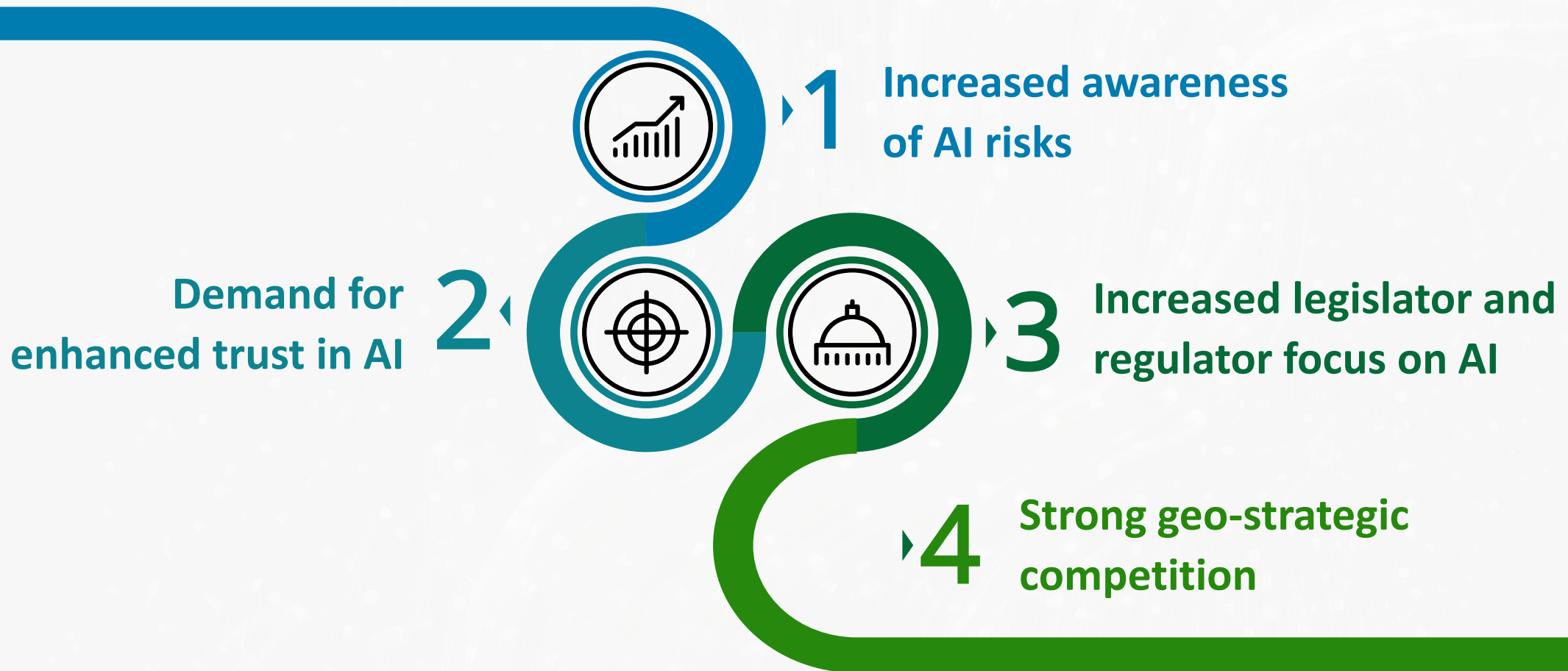
Companies that „wait and see“ will
be left behind as enterprises see
early results due to AI

Apple's 'sexist' credit card investigated
by US regulator

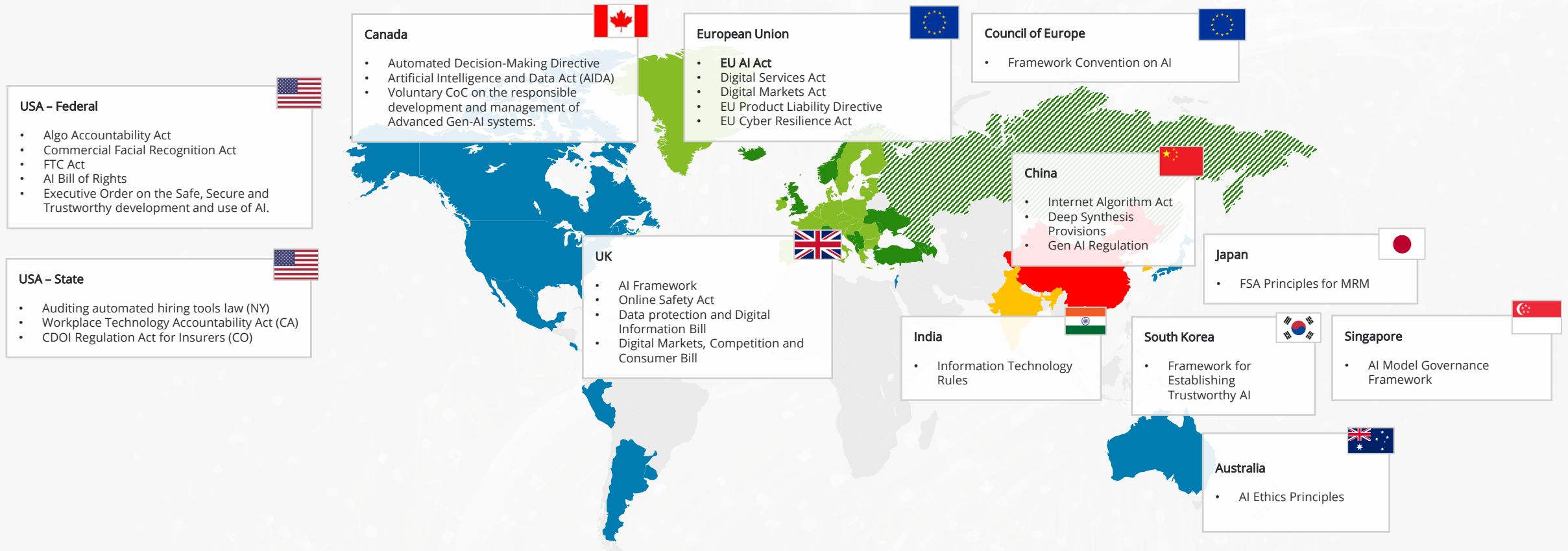
HEALTH AND HUMAN SERVICES

Nurses Worry About Lack of AI Rules in Hospitals

Perception of AI



Regulatory activities on AI



The EU AI Act - Fostering Trustworthy AI

GOALS

AI systems on the Union market are **safe, secure, and respect fundamental rights** and EU **values**.

MARKET

A level playing field in the EU **single market**.

FRAMEWORK

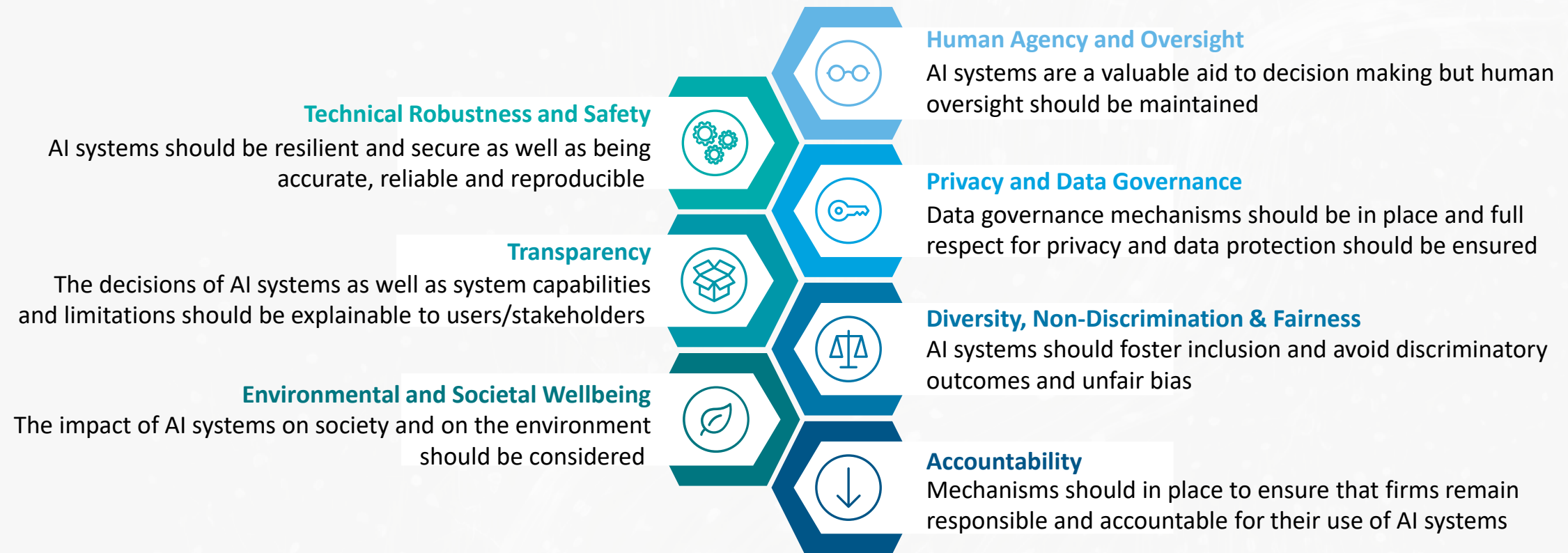
Governance and effective enforcement of requirements applicable to AI systems.

RULES

Foster **innovation and investment** in safe and trustworthy AI.

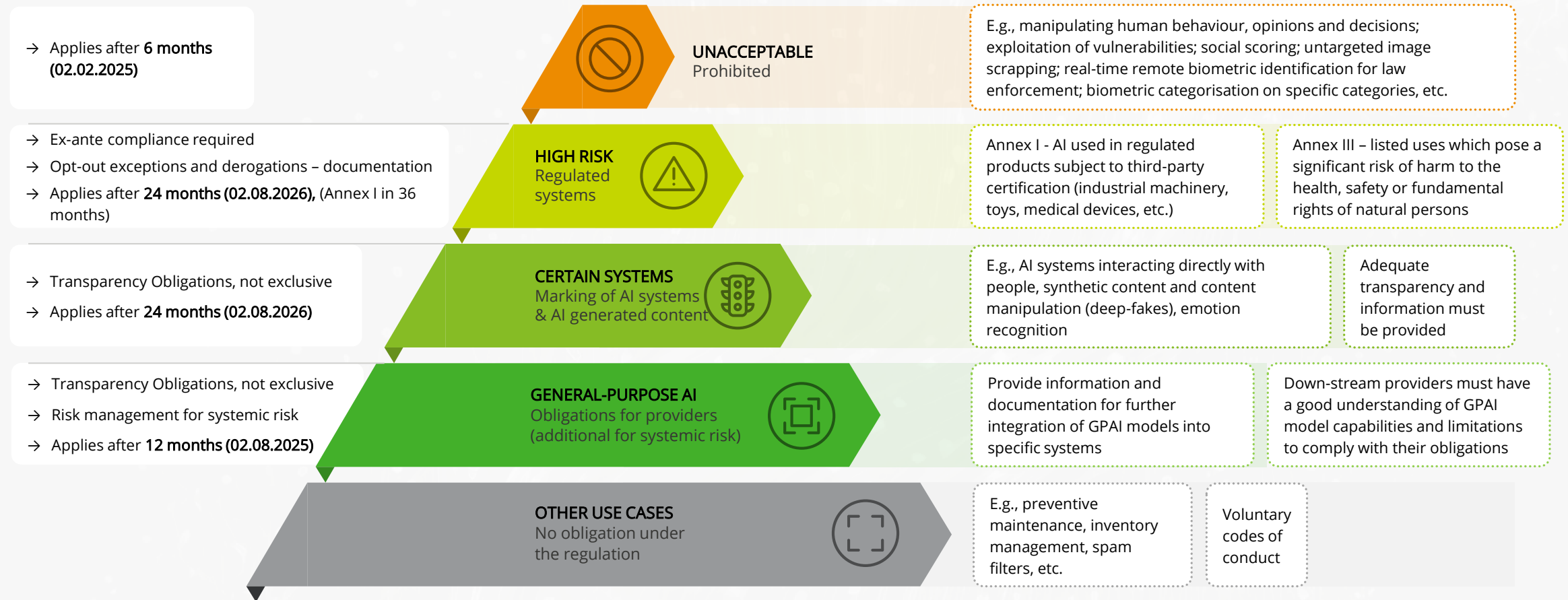
Principles for achieving Trustworthy AI (EU HLEG)

The guidelines for *Trustworthy AI* are at the heart of proposed EU AI Act. The framework is built on the fundamental principles of lawfulness, ethics and robustness with the purpose of creating AI systems within the boundaries of ethical standards.



Risk-based and proportionate

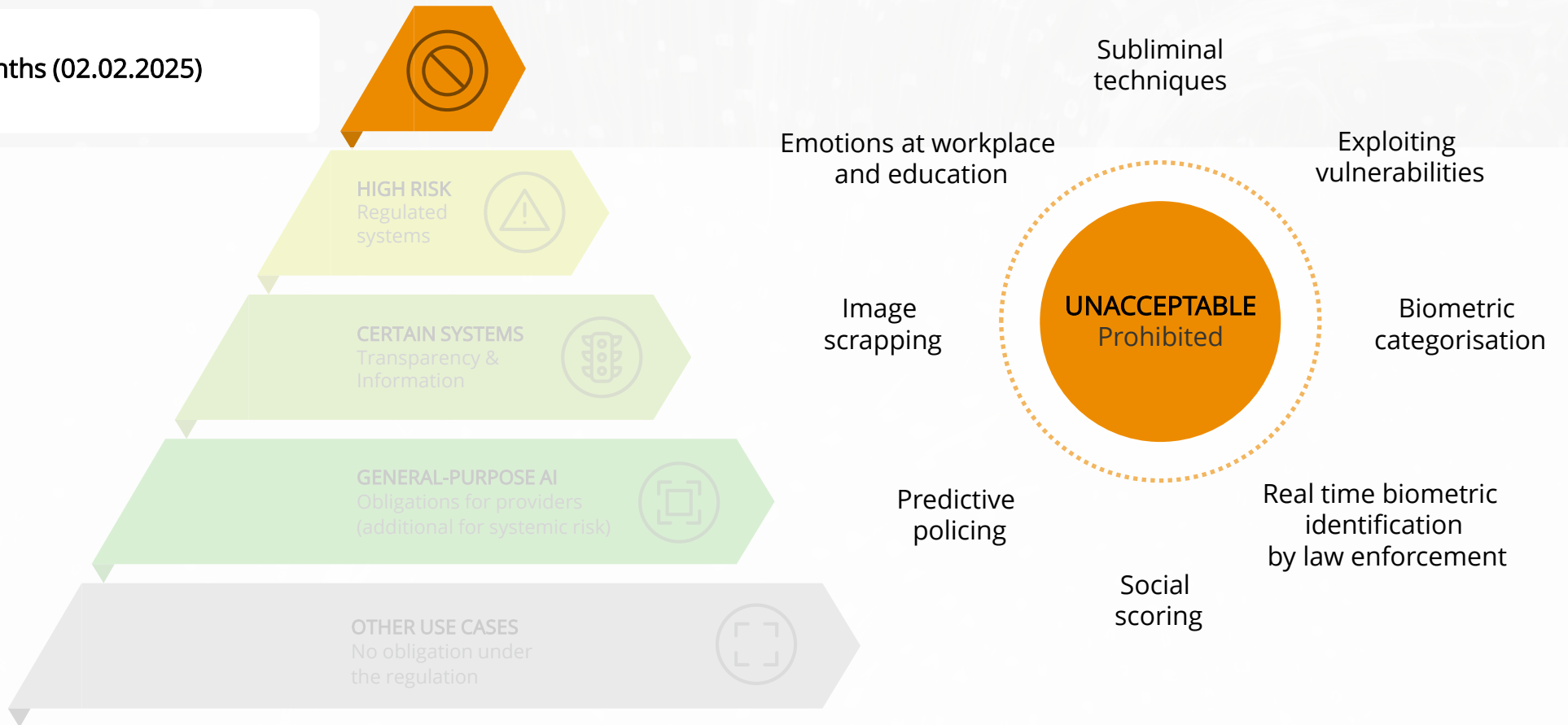
The development and use of new technologies will be subjected to a **risk-based and proportionate approach**, and the new requirements will apply to all actors along the AI value chain and lifecycle, including developers and users.



Risk-based and proportionate

Practices which are particularly harmful and abusive should be **prohibited** because they contradict Union values.

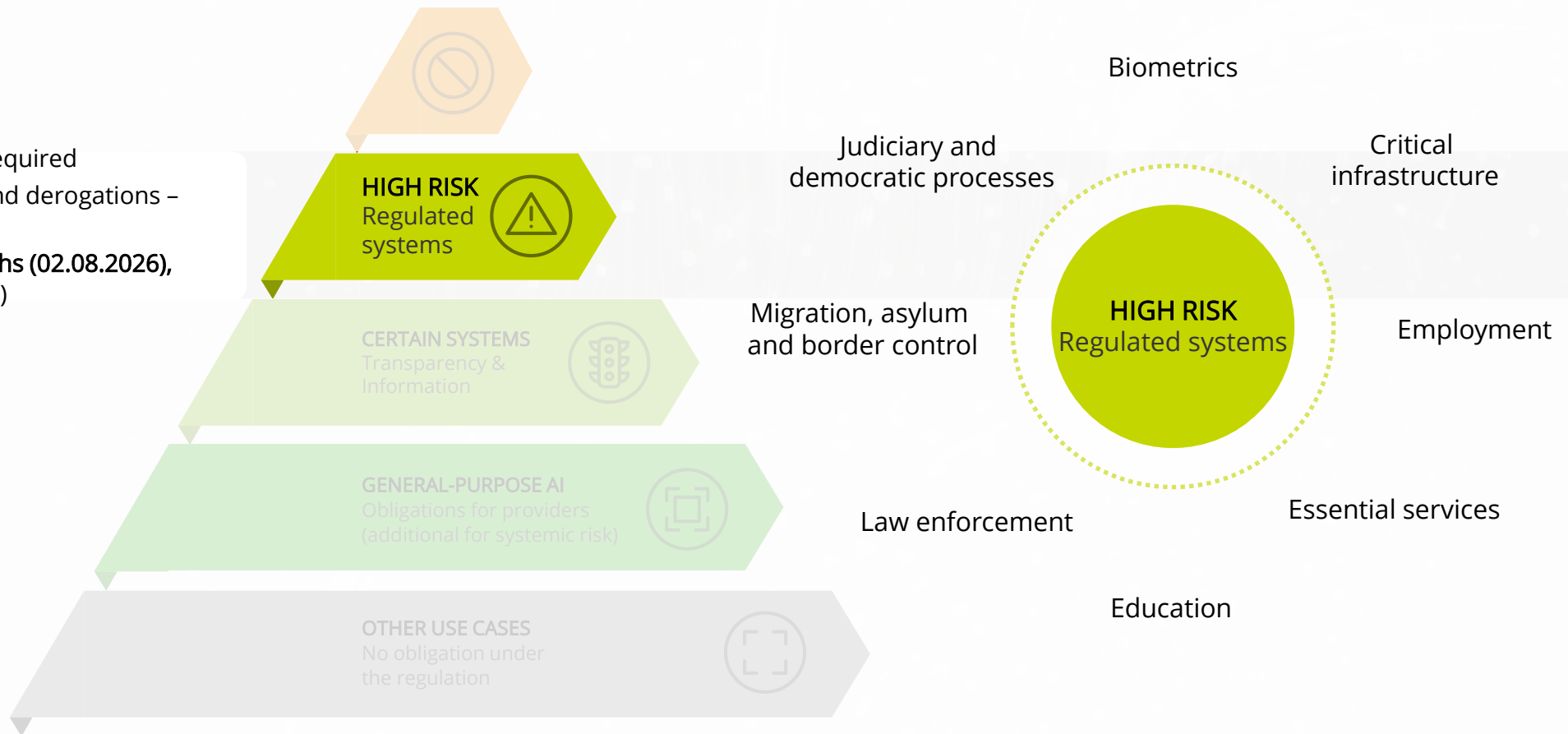
→ Applies after 6 months (02.02.2025)



Risk-based and proportionate

High-risk AI systems should only be placed on the Union market, put into service or used if they comply with certain mandatory requirements.

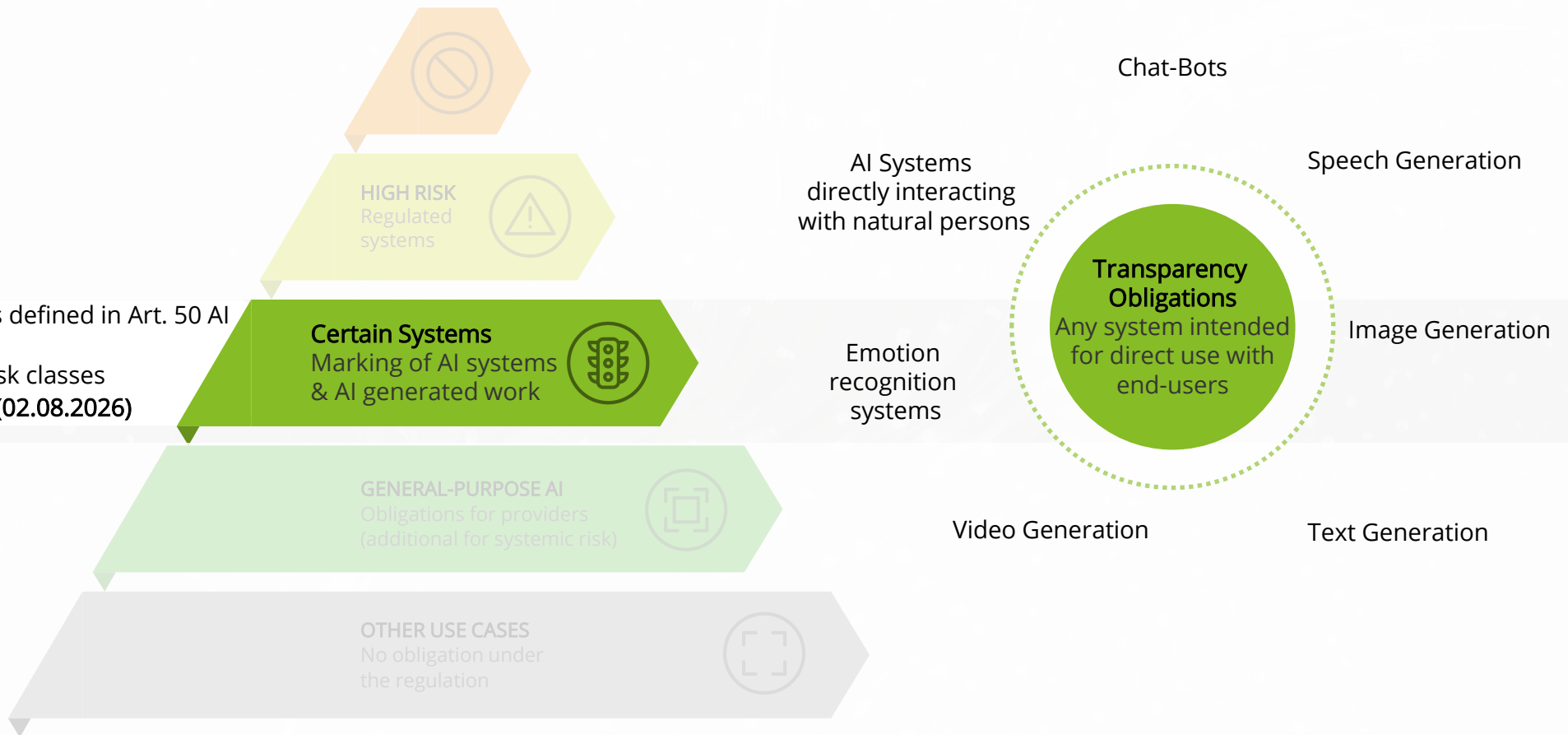
- Ex-ante compliance required
- Opt-out exceptions and derogations – documentation
- Applies after **24 months (02.08.2026)**, (Annex I in 36 months)



Risk-based and proportionate

AI Systems and GPAI Models, capable of generating new work, manipulating existing work, biometric or emotional categorization, or which are directly interacting with natural persons, are subject to **Transparency Obligations**.

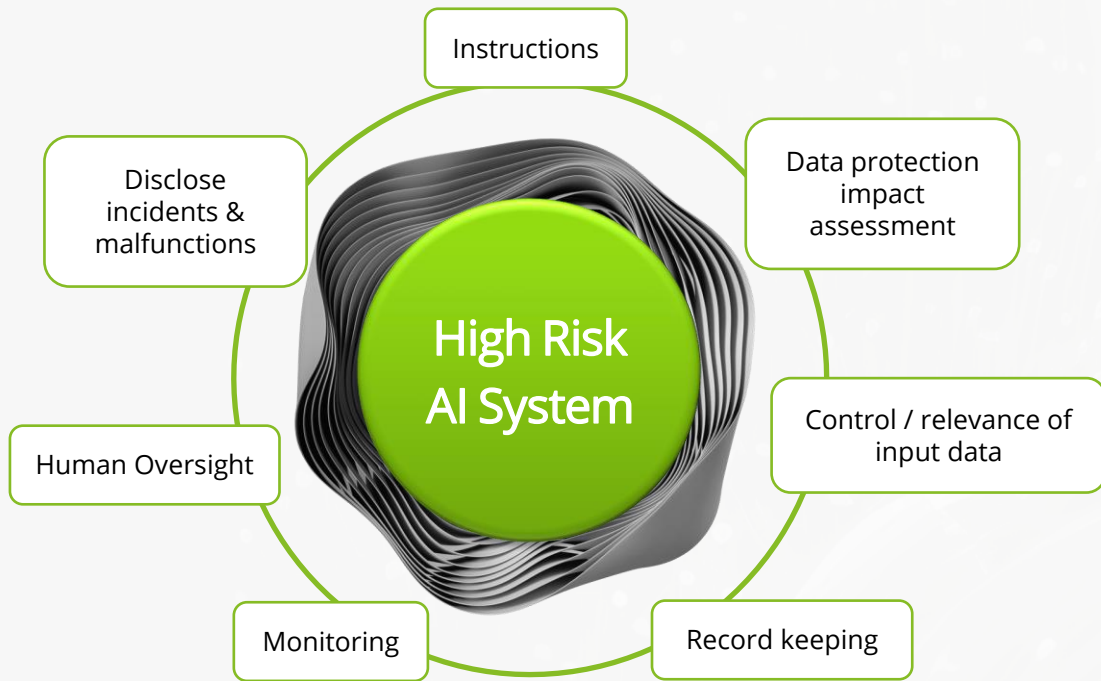
- Transparency obligations defined in Art. 50 AI Act
- Non-exclusive to other risk classes
- Applies after **24 months (02.08.2026)**



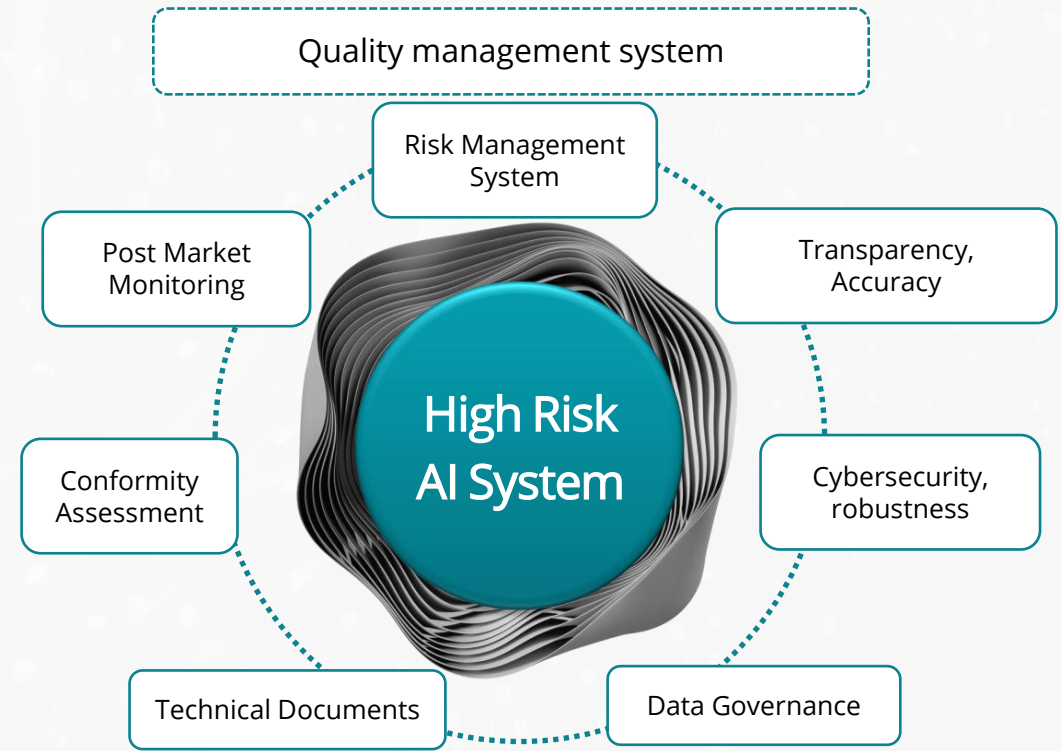
How will it affect companies?

Compliance with the AI Act will be a condition for the placing of AI systems on the market, their putting into service or use.

Requirements* for Deployers



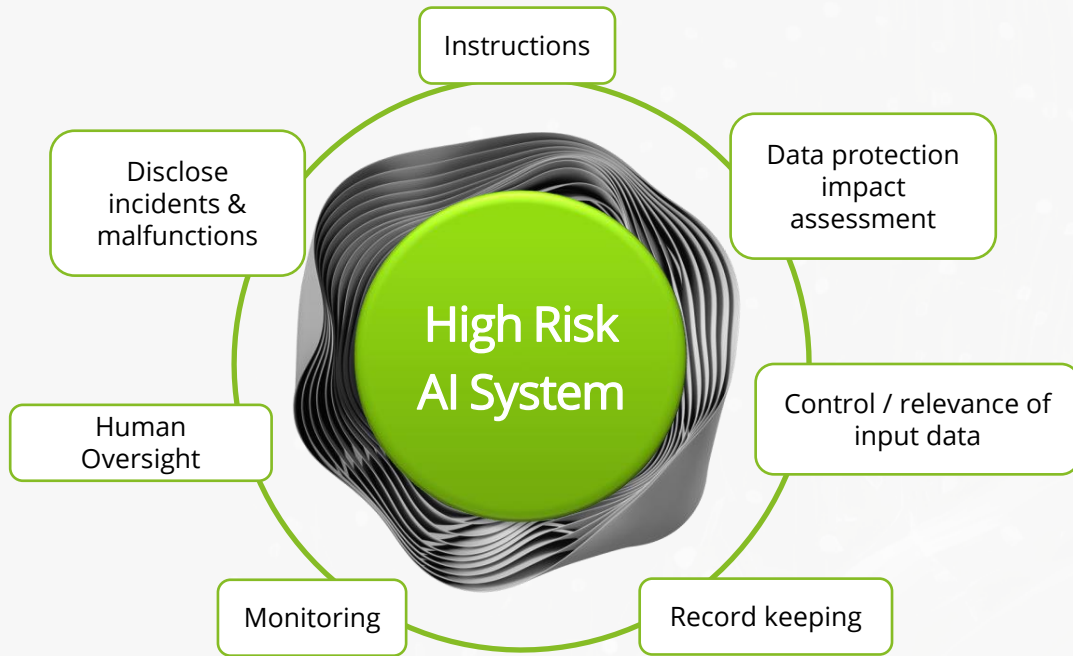
Additional Requirements* for Providers



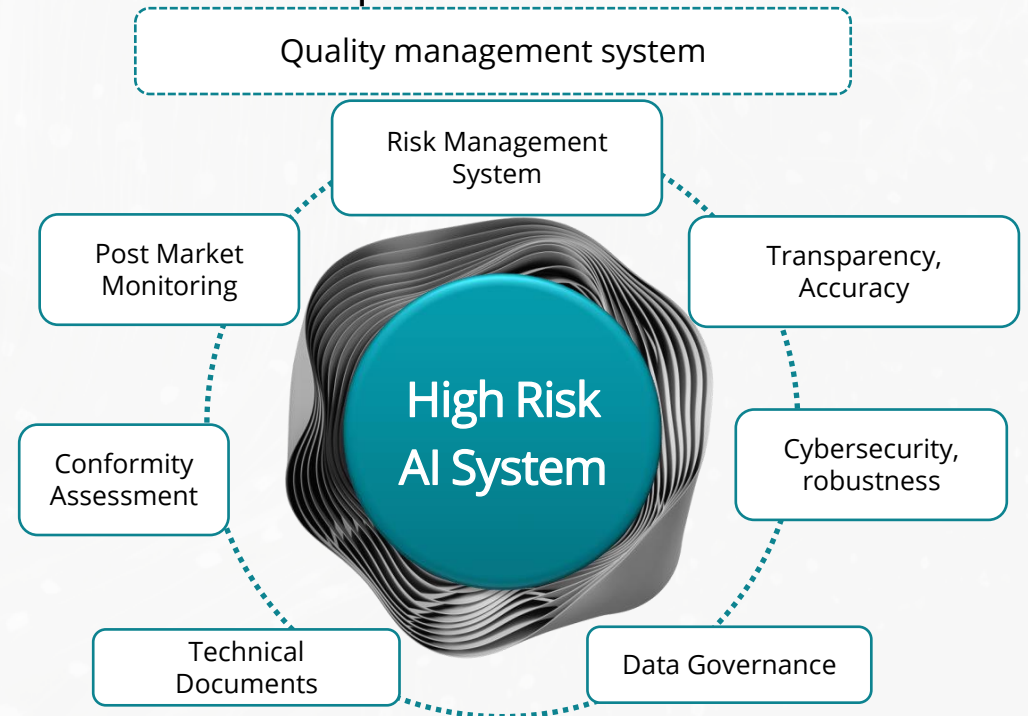
How will it affect companies?

Compliance with the AI Act will be a condition for the placing of AI systems on the market, their putting into service or use.

Requirements* for Deployers



Additional Requirements* for Providers



Enforcement and penalties

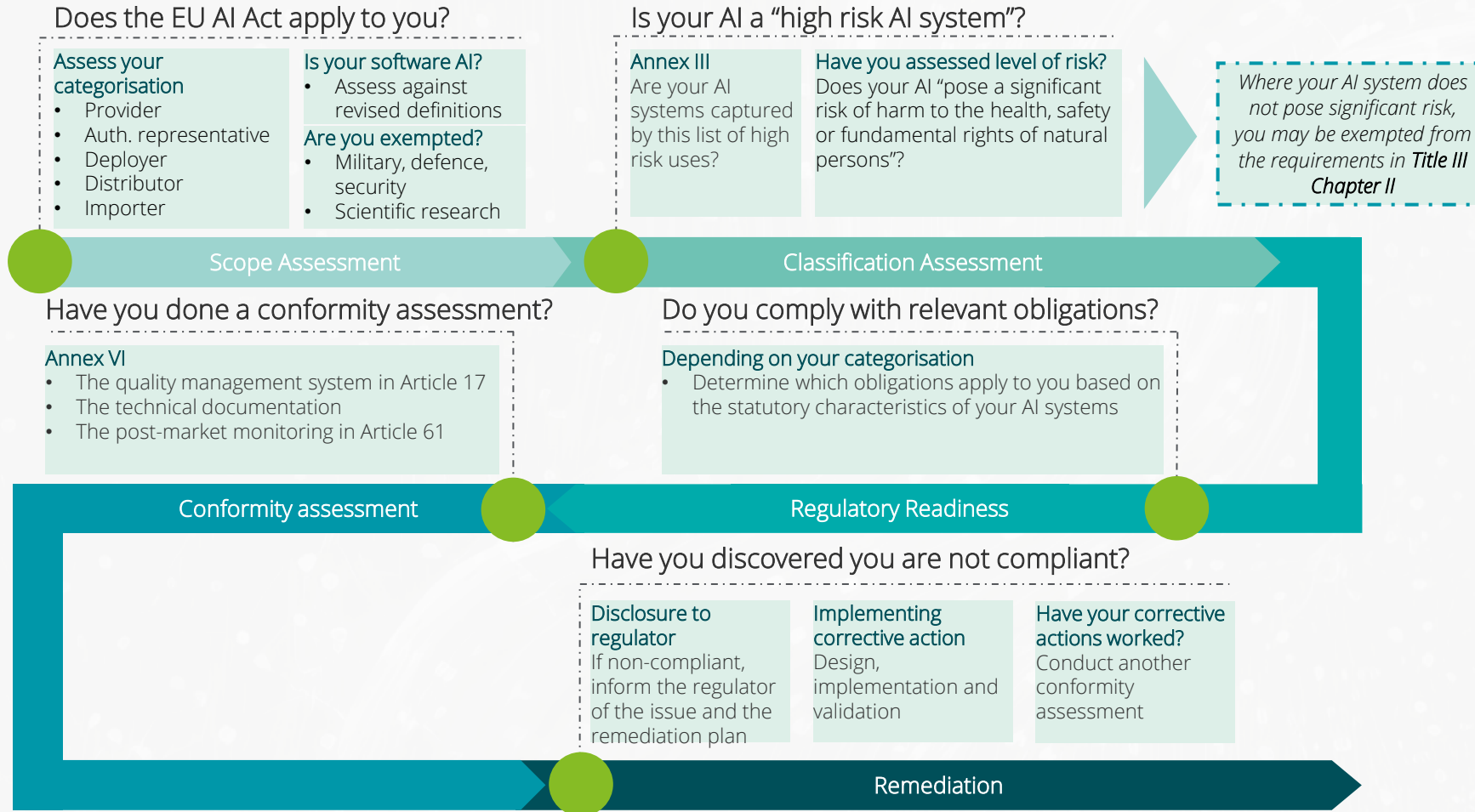
Prohibited practices
<35 MIO EUR or 7%

Other non-compliance
<15 MIO EUR or 3%

Incorrect, incomplete or misleading
<7.5 MIO EUR or 1%

What are the steps towards compliance?

The transition period requires AI system deployers to identify the AI systems they are using and assess their conformity without further delay to prevent potential non-compliance.



Was jetzt zu tun ist

Kurzfristige Maßnahmen für die Interne Revision

01

Update Prüfprogramm KI Governance

Aktualisieren Sie ggf. Ihr Vorgehen zur Prüfung der KI-Governance in Ihrem Unternehmen. Dies sollte auch eine Überprüfung der KI-Strategie, der jeweiligen Business Cases und inwieweit KI-Risiken berücksichtigt wurden, umfassen. Es sollte geprüft werden, inwieweit das Top Management in die Definition der KI-Strategie und den damit verbundenen Leitplanken eingebunden waren/sind, da diese organisationsweite Konsequenzen haben können.

02

Bestandsaufnahme und Review relevanter Richtlinien

Die Revision sollte in Erwägung ziehen, alle von der Organisation entwickelten KI-Richtlinien zu sichten, einschließlich der Leitlinien für die zulässige Nutzung und/oder der Richtlinien, die Parameter für die Entwicklung von KI-Systemen festlegen.

03

AI Inventory / KI Inventur

Liegt eine vollständige Übersicht der KI-Systeme und Anwendungsfälle vor? Das AI Inventory sollte aktive und in der Entwicklung befindliche KI-Projekte mit Einzelheiten zu deren Status und Risikoüberlegungen umfassen - letztlich können KI-Risiken nur dann gemanagt werden, wenn Klarheit über den KI-Einsatz besteht.

04

Regulatory readiness

Schaffen Sie Transparenz darüber, ob und wie Ihr Unternehmen mit dem sich schnell verändernden regulatorischen Umfeld Schritt hält. Unternehmen müssen die Vorschriften in allen Regionen, in denen sie tätig sind, berücksichtigen. Bei nicht vollständiger Erfassung relevanter Regulatorik, besteht die Gefahr, dass sie bereits eingeführte KI-Nutzungsfälle einfrieren müssen, was zu erheblichen Geschäftsunterbrechungen führen könnte.

05






Anpassung Risikomanagement

Bestehende Risikomanagementprozesse müssen möglicherweise angepasst werden, um die mit KI verbundenen Risiken angemessen abzudecken. Derzeit entwickelte Methoden für Risikomanagement und Risikobewertungen für KI sollten in bestehende Risikomanagementprozesse integriert werden. Auch Erklärungen zum Risikoappetit und Risikotoleranz müssen möglicherweise aktualisiert werden. Viele Organisationen passen außerdem bestehende Richtlinien an, um für KI gewappnet zu sein, z. B. KI-Ethikbeiräte und die Einrichtung von KI-Exzellenzzentren.

Summary – Discussion points

AI, a powerful technique that comes with manageable risks and regulatory obligations

Key areas

- Trustworthy AI & EU AI Act 
- Setting up Governance structures 
- Auditing AI & Model validation 
- Monitoring and issue logging 
- AI as an audit & support mechanism 

Key aspects

- 
 - Obligations depending on risk category
 - TAI - full AI lifecycle process to control risks
- 
 - Three lines of defense
 - Applying AI governance structure to operationalize AI
- 
 - Risk assessment, Internal Control, AI model inspection, management communication, issue resolution
- 
 - Fully integrated AI risk management monitoring
 - Cross AI Lifecycle handling of issues and compliance
- 
 - Diverse anomaly detection methods to identify fraudulent patterns
 - GenAI for efficient report interaction and generation



About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Legal means the legal practices of DTTL member firms, their affiliates or their related entities that provide legal services. The exact nature of these relationships and provision of legal services differs by jurisdiction, to allow compliance with local laws and professional regulations. Each Deloitte Legal practice is legally separate and independent, and cannot obligate any other Deloitte Legal practice. Each Deloitte Legal practice is liable only for its own acts and omissions, and not those of other Deloitte Legal practices. For legal, regulatory and other reasons, not all member firms, their affiliates or their related entities provide legal services or are associated with Deloitte Legal practices.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s more than 345,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2024. For information, contact Deloitte Global.