



SHAPING EUROPE'S DIGITAL FUTURE

AI is good ...

- For citizens
- For business
- For the public interest



... but creates some risks

- For the safety of consumers and users
- For fundamental rights

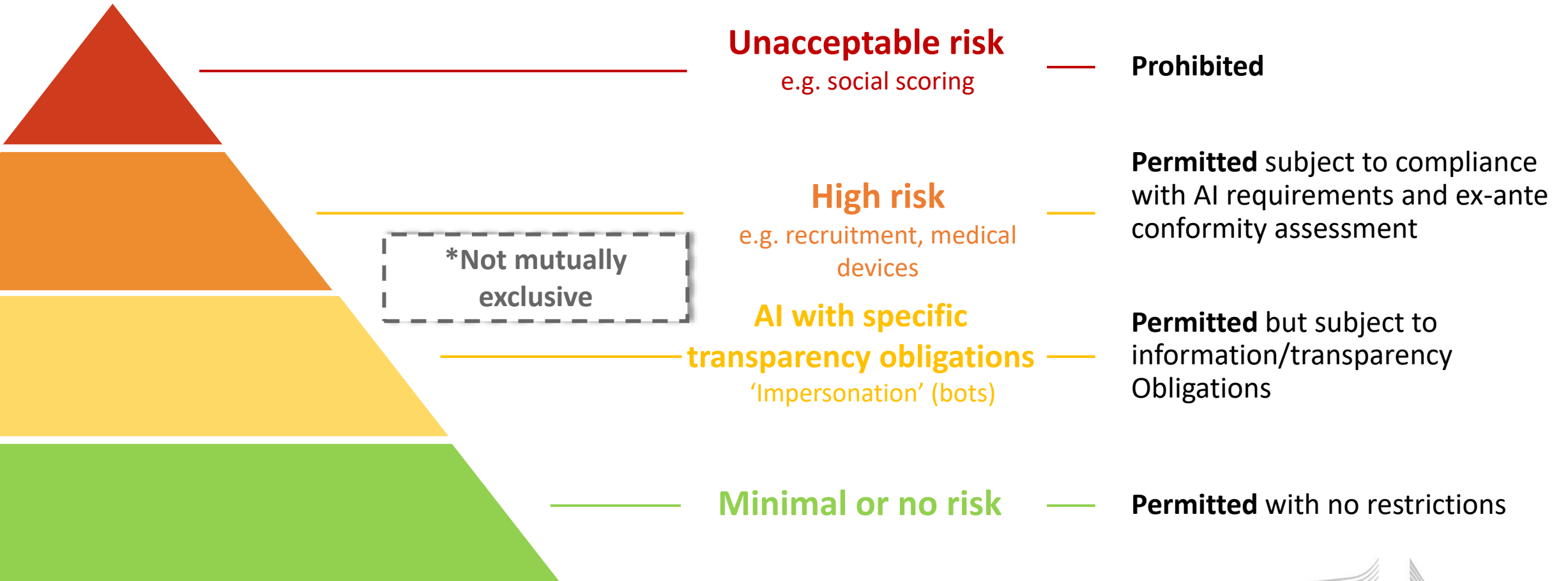
Definition and technological scope of the regulation (Art. 3)

Definition of Artificial Intelligence

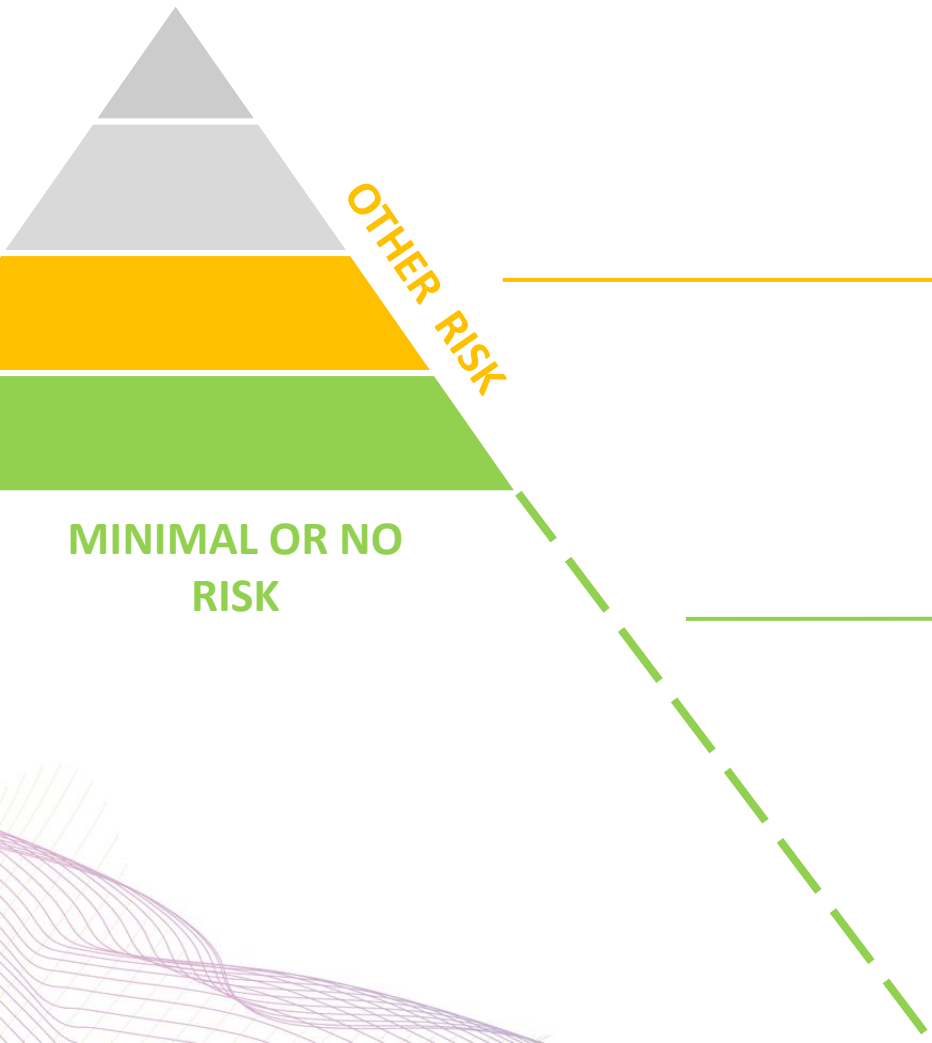
- ▶ Definition of AI should be **as neutral as possible** in order to cover techniques which are not yet known/developed
- ▶ **Overall aim is to cover all AI**, including traditional symbolic AI, Machine learning, as well as hybrid systems
- ▶ **Annex I**: list of AI techniques and approaches should provide for legal certainty (adaptations over time may be necessary)

“a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with”

A risk-based approach to regulation



Most AI systems will not be high-risk (Titles IV, IX)



New transparency obligations for certain AI systems (Art. 52)

- ▶ **Notify humans** that they are **interacting with an AI system** unless this is evident
- ▶ Notify humans that emotional recognition or biometric categorisation systems are applied to them
- ▶ Apply **label to deep fakes** (unless necessary for the exercise of a fundamental right or freedom or for reasons of public interests)

Possible voluntary codes of conduct for AI with specific transparency requirements (Art. 69)

- ▶ No mandatory obligations
- ▶ Commission and Board to encourage drawing up of codes of conduct intended to foster the **voluntary application of requirements to low-risk AI systems**

High-risk Artificial Intelligence Systems (Title III, Annexes II and III)

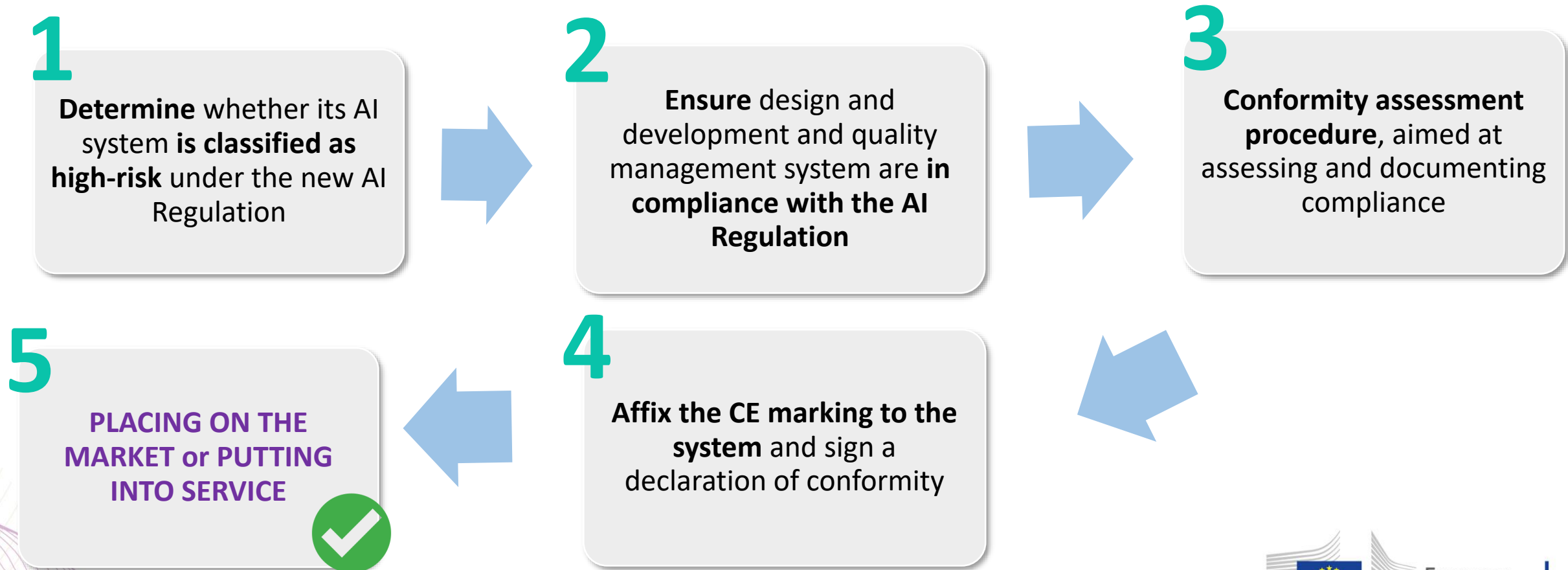


Certain applications in the following fields:

- 1 SAFETY COMPONENTS OF REGULATED PRODUCTS**
(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation
- 2 CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING FIELDS**
 - ✓ Biometric identification and categorisation of natural persons
 - ✓ Management and operation of critical infrastructure
 - ✓ Education and vocational training
 - ✓ Employment and workers management, access to self-employment
 - ✓ Access to and enjoyment of essential private services and public services and benefits
 - ✓ Law enforcement
 - ✓ Migration, asylum and border control management
 - ✓ Administration of justice and democratic processes

CE marking and process (Title III, chapter 4, art. 49.)

CE marking is an indication that a product complies with the requirements of a relevant Union legislation regulating the product in question. In order to affix a CE marking to a high-risk AI system, a provider shall undertake **the following steps**:



Requirements for high-risk AI (Title III, chapter 2)

Establish and
implement **risk
management**
processes

&
In light of the
**intended
purpose** of the
AI system

Use high-quality **training, validation and testing data** (relevant, representative etc.)

Establish **documentation** and design logging features (traceability & auditability)

Ensure appropriate certain degree of **transparency** and provide users with **information**
(on how to use the system)

Ensure **human oversight** (measures built into the system and/or to be implemented by users)

Ensure **robustness, accuracy** and **cybersecurity**

AI that contradicts EU values is prohibited (Title II, Article 5)

X

Subliminal manipulation
resulting in physical/
psychological harm

Example: An **inaudible sound** is played in truck drivers' cabins to push them to **drive longer than healthy and safe**. AI is used to find the frequency maximising this effect on drivers.

X

**Exploitation of children
or mentally disabled persons**
resulting in physical/psychological harm

Example: A doll with an integrated **voice assistant** encourages a minor to **engage in progressively dangerous behavior** or challenges in the guise of a fun or cool game.

X

**General purpose
social scoring**

Example: An AI system **identifies at-risk children** in need of social care **based on insignificant or irrelevant social 'misbehavior'** of parents, e.g. missing a doctor's appointment or divorce.

X

**Remote biometric identification for law
enforcement purposes in publicly accessible
spaces (with exceptions)**

Example: All faces captured live by video cameras checked, in real time, against a database to identify a terrorist.

Remote biometric identification (RBI) (Title II, Art. 5, Title III)

Use of real-time RBI systems for law enforcement (Art. 5)



Prohibition of use for law enforcement purposes in publicly accessible spaces with exceptions:

- Search for victims of crime
- Threat to life or physical integrity or of terrorism
- Serious crime (EU Arrest Warrant)

Ex-ante authorisation by judicial authority or independent administrative body

Putting on the market of RBI systems (real-time and ex-post)



➤ **Ex ante third party conformity assessment**

- Enhanced logging requirements
- “Four eyes” principle

No additional rules foreseen for use of real-time and post RBI systems: existing data protection rules apply

Supporting innovation (Title V)

**Regulatory
sandboxes
Art. 53 and 54**

**Support for
SMEs/start-ups
Art. 55**



The governance structure (Titles VI and VII)

European level

European Commission to act
as Secretariat

Artificial Intelligence
Board



Expert Group*



National level

National Competent
Authority/ies



*Not foreseen in the regulation but the Commission intends to introduce it in the implementation process



Thank you