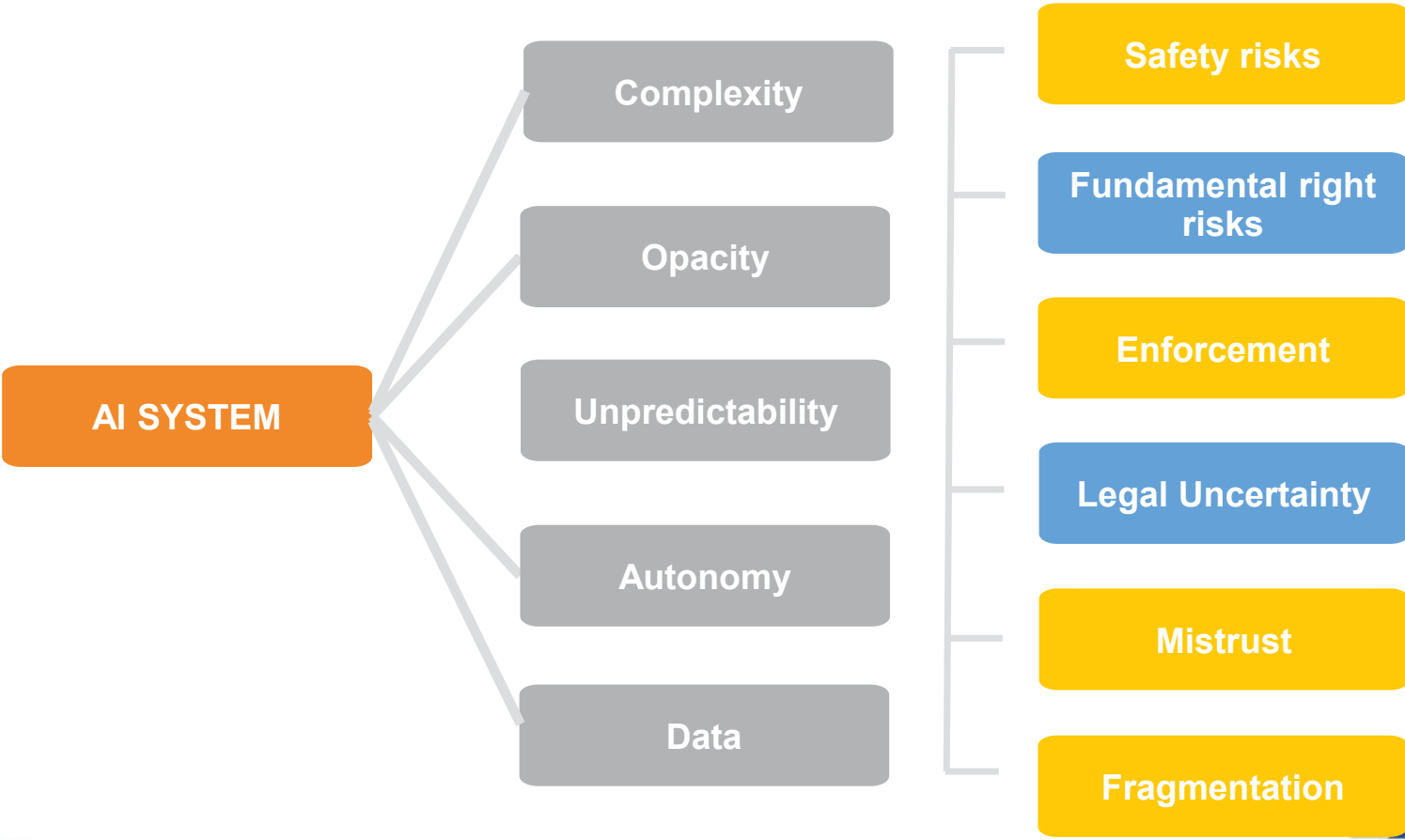




# SHAPING EUROPE'S DIGITAL FUTURE

# Why do we regulate AI use cases?



# 1. Proposal for a legal framework on AI

# Scope of application (Art. 2)

## Regulation applicable to:

- ▶ **Providers (public or private)** placing on the market or putting into service AI systems in the Union independent from their origin
- ▶ **Users (public or private)** located within the Union
- ▶ **Providers and users** located in a third country, where the output produced by the system is used in the Union

## Excluded from the scope:

- ▶ Public authorities in a third country or international organisations who use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States
- ▶ AI developed or used exclusively for military purposes

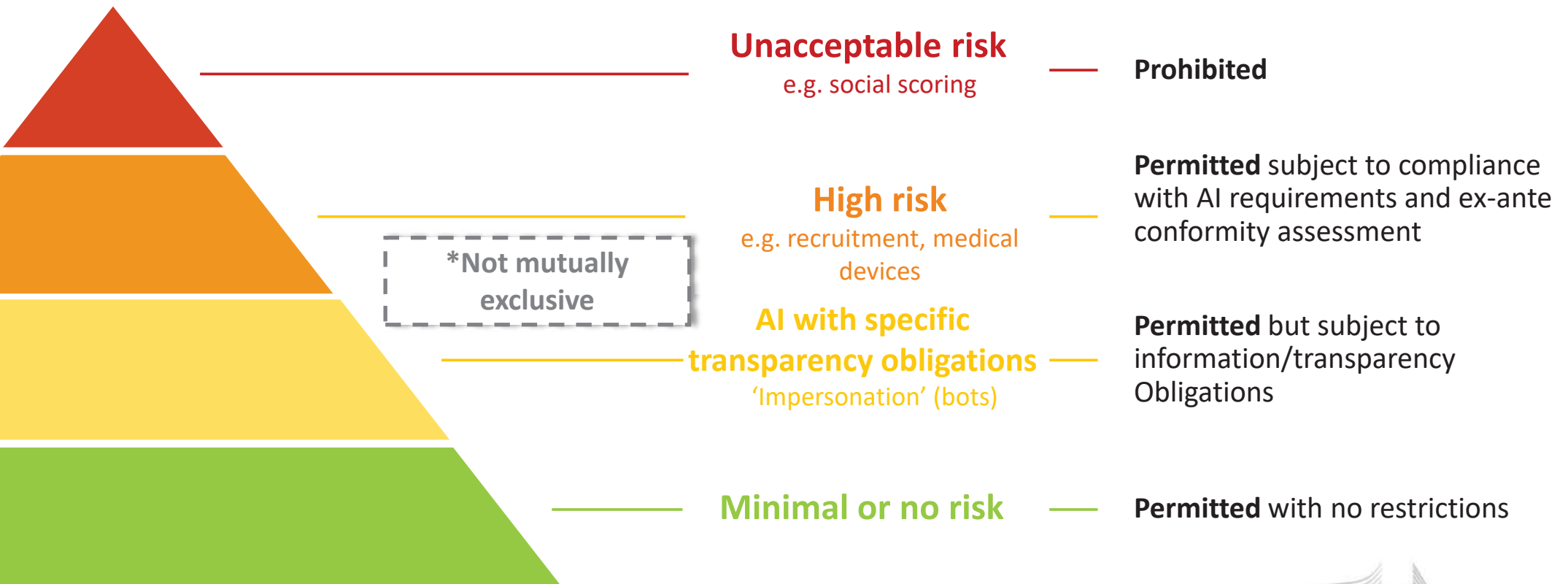
# Definition and technological scope of the regulation (Art. 3)

## 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



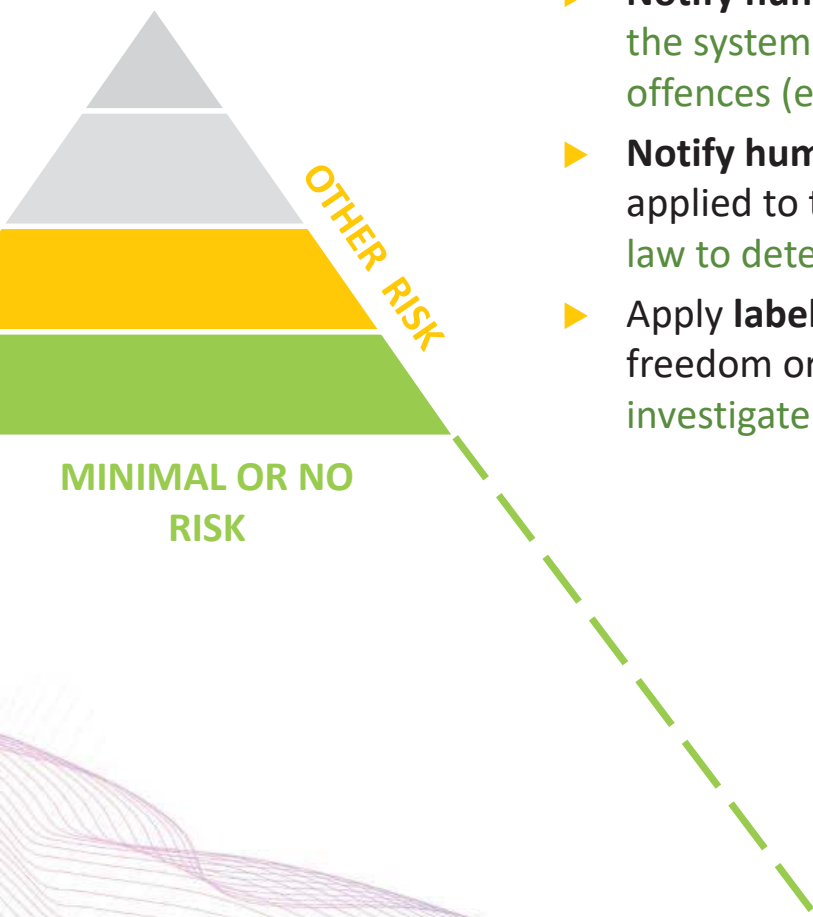
# Most AI systems will not be high-risk (Titles IV, IX)

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

- ▶ **Notify humans** that they are **interacting with an AI system** unless this is evident or the system is authorised by law to detect, prevent, investigate and prosecute criminal offences (exception: system for the public to report a criminal offence).
- ▶ **Notify humans** that **emotional recognition or biometric categorisation systems** are applied to them unless the system is used for biometric categorisation, permitted by law to detect, prevent and investigate criminal offences
- ▶ Apply **label to deep fakes** unless necessary for the exercise of a fundamental right or freedom or for reasons of public interests or authorised by law to detect, prevent, investigate and prosecute criminal offences

## 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



# High-risk Artificial Intelligence Systems in Law Enforcement (Annex III)

AI systems intended to be used by law enforcement authorities (for )

- making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
- predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;
- profiling of natural persons in the course of detection, investigation or prosecution of criminal offences;
- crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data;
- polygraphs and similar tools or to detect the emotional state of a natural person;
- to detect deep fakes;
- evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences.

## High-risk systems in Migration, asylum and border control management:

AI systems intended to be used by competent public authorities

- as polygraphs and similar tools or to detect the emotional state of a natural person;
- to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;
- for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;
- for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

# 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**

# Overview: obligations of operators (Title II, Chapter 3)



## Provider obligations

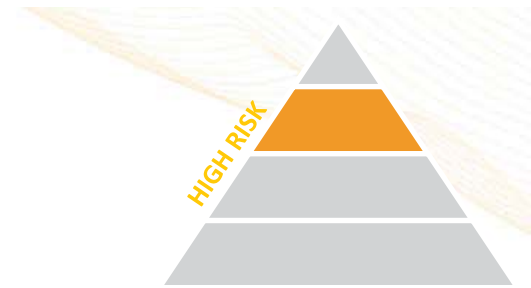
- ▶ Establish and Implement **quality management** system in its organisation
- ▶ Draw-up and keep up to date **technical documentation**
- ▶ **Logging** obligations to enable users to monitor the operation of the high-risk AI system
- ▶ Undergo **conformity assessment** (self assessment for law enforcement AI systems and involvement of market surveillance authorities for remote biometric identification systems) and potentially re-assessment of the system (in case of significant modifications)
- ▶ Register AI system in EU database (no publication of the instruction of use for HOME policies, Annex VIII, 11.)
- ▶ Affix CE marking and sign declaration of conformity
- ▶ Conduct **post-market monitoring**
- ▶ **Collaborate** with market surveillance authorities (data protection or supervisory authority, Art. 63(5))

## User obligations

- ▶ Operate AI system in accordance with **instructions of use**
- ▶ Ensure **human oversight** when using of AI system
- ▶ **Monitor** operation for possible risks
- ▶ **Inform the provider or distributor about any serious incident** or any malfunctioning
- ▶ **Existing legal obligations** continue to apply (e.g. under GDPR)



# Lifecycle of AI systems and relevant obligations



## Design in line with requirements



Ensure AI systems **perform consistently for their intended purpose** and are in **compliance with the requirements** put forward in the Regulation

## Conformity assessment



**Ex ante** conformity assessment when the AI system is used or placed on the market in Europe

## Post-market monitoring



Providers to **actively and systematically collect, document and analyse relevant data** on the reliability, performance and safety of AI systems throughout their lifetime, and to **evaluate continuous compliance of AI systems with the Regulation**

## Incident report system



**Report serious incidents as well as malfunctioning leading to breaches to fundamental rights** (as a basis for investigations conducted by competent authorities).

## New conformity assessment



**New conformity assessment** in case of **substantial modification** (modification to the intended purpose or change affecting compliance of the AI system with the Regulation) by providers or any third party, including when changes are **outside the “predefined range”** indicated by the provider for **continuously learning AI systems**.

# 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 - Art. 6, Annex 3 (1)(a))

## Use of real-time RBI systems for law enforcement purposes (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 post, public and private)



➤ **Requirements for high-risk systems**

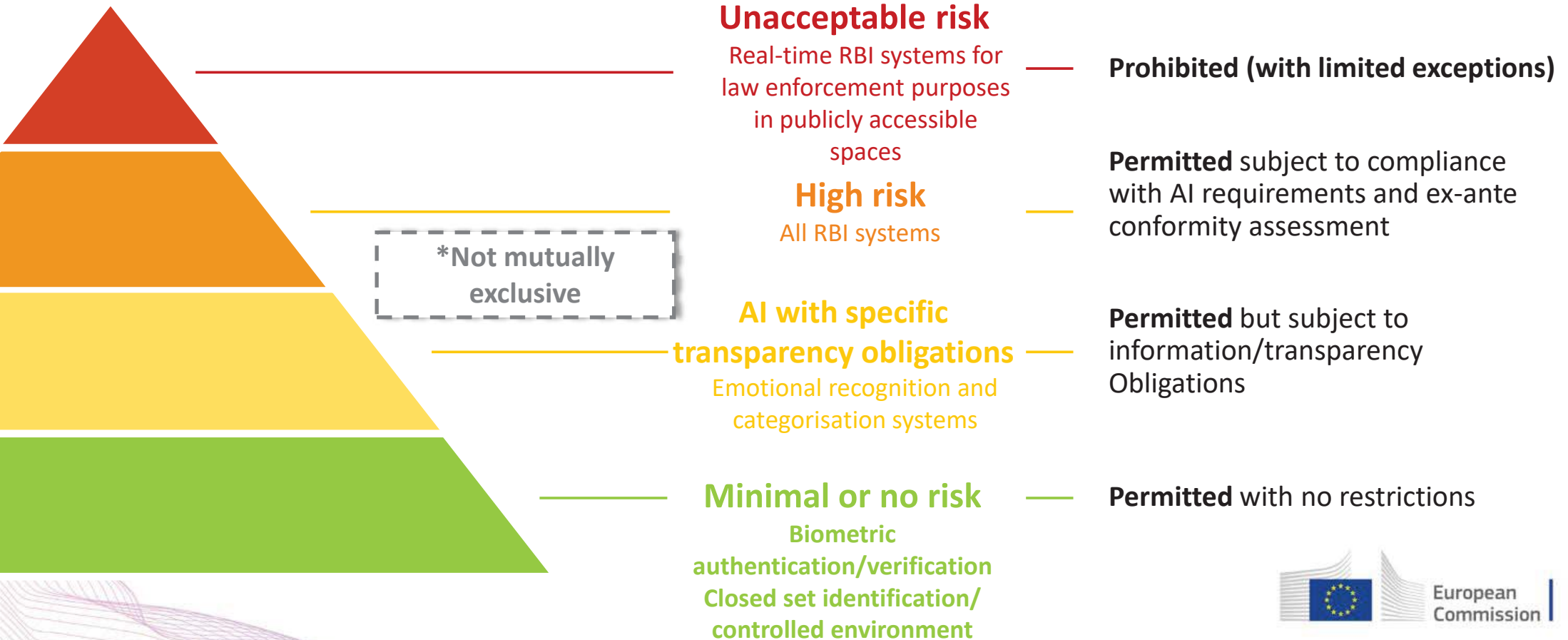
➤ **Ex ante third party conformity assessment** by market surveillance authority

➤ Enhanced logging requirements

➤ “Four eyes” principle

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

# A risk-based approach to regulation






# 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 

- ▶ **For law enforcement:** MS to designate data protection or sectoral supervisory authority, Art. 63(5)
- ▶ Special rules on **confidentiality of information** Art. 70 (2)

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

# Supporting innovation (Title V)

**Regulatory  
sandboxes  
Art. 53 and 54**

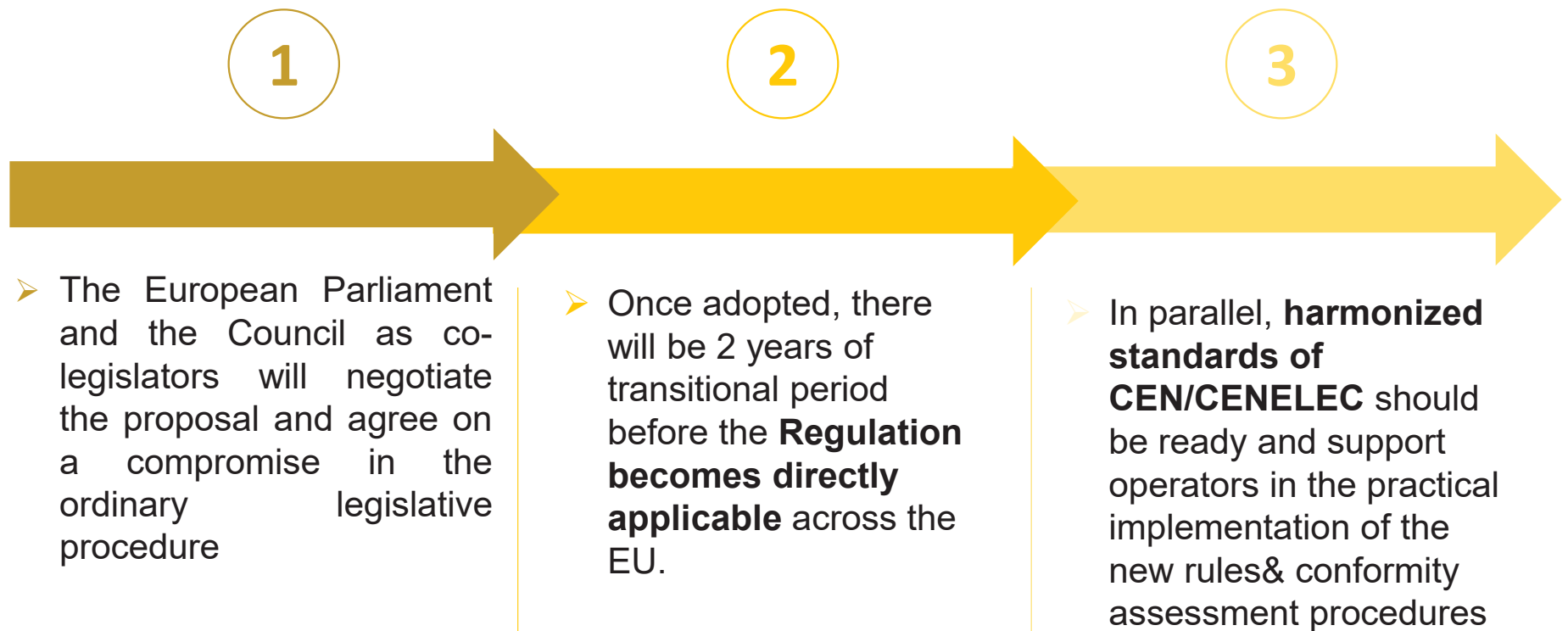
**Support for  
SMEs/start-ups  
Art. 55**



**Art. 54(1)(a)(i)  
Further processing of personal data for  
development of AI systems for law  
enforcement purposes**



# Next steps



# The Coordinated Plan on AI 2021 review

The Coordinated Plan represents a joint commitment between the Commission and Member States that by working together, Europe can maximise its AI potential to compete globally

## The Coordinated Plan 2018

- ▶ Some **70 individual forward-looking actions**
- ▶ Developed together with the **Member States**
- ▶ Member States were encouraged to develop **national AI strategies**
- ▶ Set up as a **rolling plan** to be updated regularly

## Why a 2021 review?

- ▶ **Covid-19 pandemic**
- ▶ **The Green Deal**
- ▶ **The RRF (+ DEP and HE) as game changer**
- ▶ **Policy alignment** with 2020 White Paper on AI (human-centric and trustworthy AI)
- ▶ **Technological developments** (new components, computing concepts, data infrastructure, new applications)
- ▶ **Lessons learned** from last two years of implementation, moving from 'intention' to 'action'

# FOUR KEY POLICY OBJECTIVES FOR ARTIFICIAL INTELLIGENCE IN EUROPE

## SET ENABLING CONDITIONS FOR AI DEVELOPMENT AND UPTAKE IN THE EU

- Acquire, pool and share policy insights
- Tap into the potential of data
- Foster critical computing capacity

## MAKE THE EU THE RIGHT PLACE; EXCELLENCE FROM LAB TO THE MARKET

- Collaboration with stakeholders, Public-private Partnership on AI, data and robotics
- Research capacities
- Testing and experimentation (TEFs), uptake by SMEs (EDIHs)
- Funding and scaling innovative ideas and solutions

## ENSURE AI TECHNOLOGIES WORK FOR PEOPLE

- Talent and skills
- A policy framework to ensure trust in AI systems
- Promoting the EU vision on sustainable and trustworthy AI in the world

## BUILD STRATEGIC LEADERSHIP IN THE SECTORS

- Climate and environment
- Health
- Strategy for Robotics in the world of AI
- Public sector
- Law enforcement, immigration and asylum
- Mobility
- Agriculture

Investments: Horizon Europe, Digital Europe, Recovery and Resilience Facility



**Thank you**