

**Excerpts from the proposal for a  
European AI Act for the  
discussion with Kilian Gross,  
European Commission,  
13 October 2021**



## Definition of “Artificial Intelligence Systems”

### Article 3

‘artificial intelligence system’ (AI system) means 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;

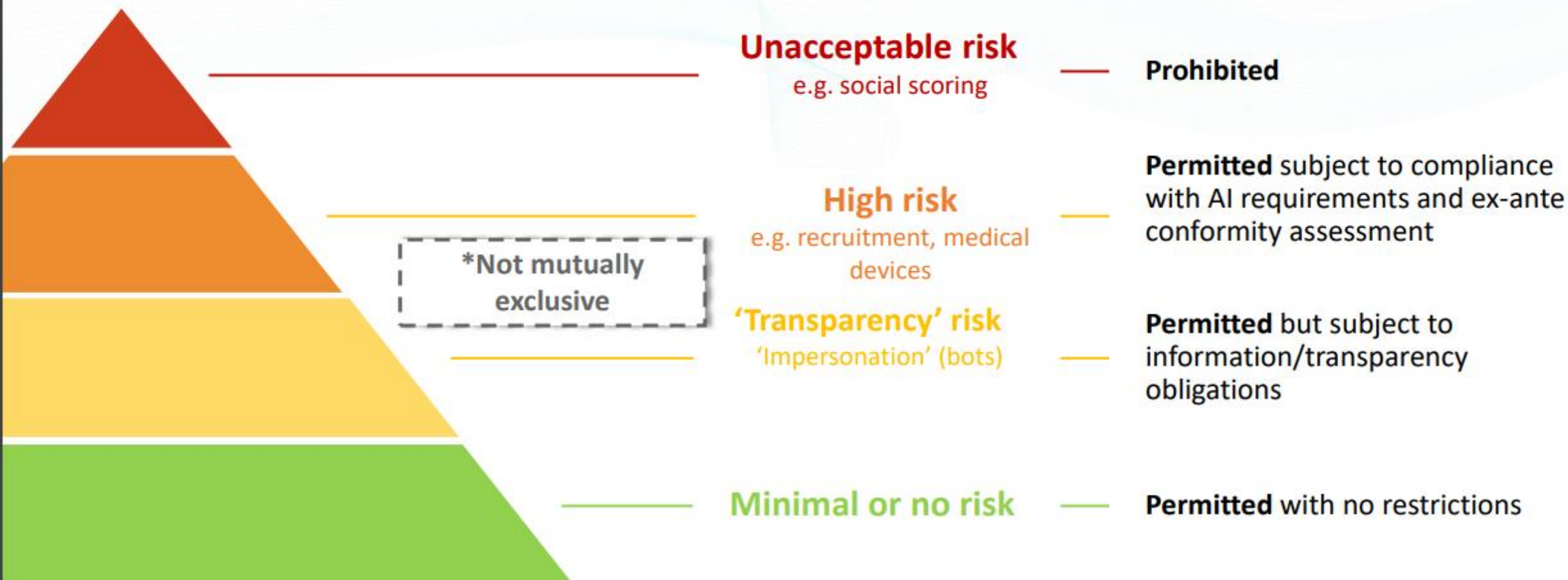
### ANNEX I

- (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- (c) Statistical approaches, Bayesian estimation, search and optimization methods.





## 2.1. Proposal for the Artificial Intelligence Act (7) Risk-based approach: an overview



*[Note: this slide is not part of AIA but taken from a presentation of the European Commission]*





*Article 52*

*Transparency obligations for certain AI systems*

1. **Providers** shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that **natural persons are informed that they are interacting with an AI system, unless this is obvious** from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.

# Transparency obligations: emotion recognition systems or biometric categorization systems

## Article 52

### *Transparency obligations for certain AI systems*

2. Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences.

From Article 3: ‘user’ means any 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;



## AI for Good | Transparency obligations: deep fakes

### *Article 52*

#### *Transparency obligations for certain AI systems*

3. **Users** of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful (**'deep fake'**), shall disclose that the content has been artificially generated or manipulated.

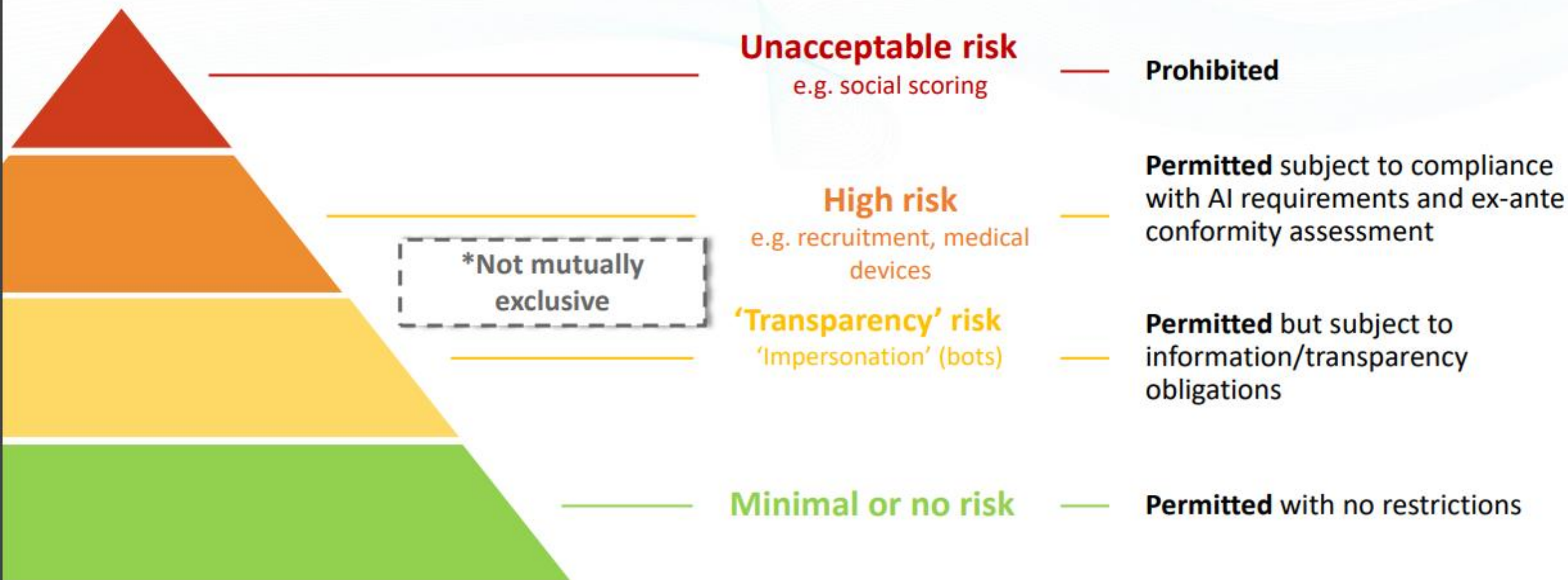
However, the first subparagraph **shall not apply** where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the **exercise of the right to freedom of expression and the right to freedom of the arts and sciences** guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.







## 2.1. Proposal for the Artificial Intelligence Act (7) Risk-based approach: an overview



*[Note: this slide is not part of AIA but taken from a presentation of the European Commission]*

### *Article 6*

#### *Classification rules for high-risk AI systems*

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:
  - (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;
  - (b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.



## High-risk AI systems – 2<sup>nd</sup> category

### Article 6

#### *Classification rules for high-risk AI systems*

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

#### ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

1. Biometric identification and categorisation of natural persons [both 'real-time' and 'post']
2. Management and operation of critical infrastructure [water, gas, heating, electricity]
3. Education and vocational training [who to attend which school/university/...; grading tests]
4. Employment, workers management and access to self-employment [hire, fire, promotion]
5. Access to and enjoyment of essential private services and public services and benefits [grant/ revoke benefits; creditworthiness; establishing priority of emergency services]
6. Law enforcement [risk assessment for (re)offending; profiling; AI as polygraphs; deep fake detection ... ]
7. Migration, asylum and border control management [AI as polygraphs; risk assessment of migrants]
8. Administration of justice and democratic processes [researching and interpreting facts]

# High-risk AI systems – Standards and Conformity Assessment

## *Article 40*


### *Harmonised standards*

High-risk AI systems which are in conformity with **harmonised standards** or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements.

## *Article 41*

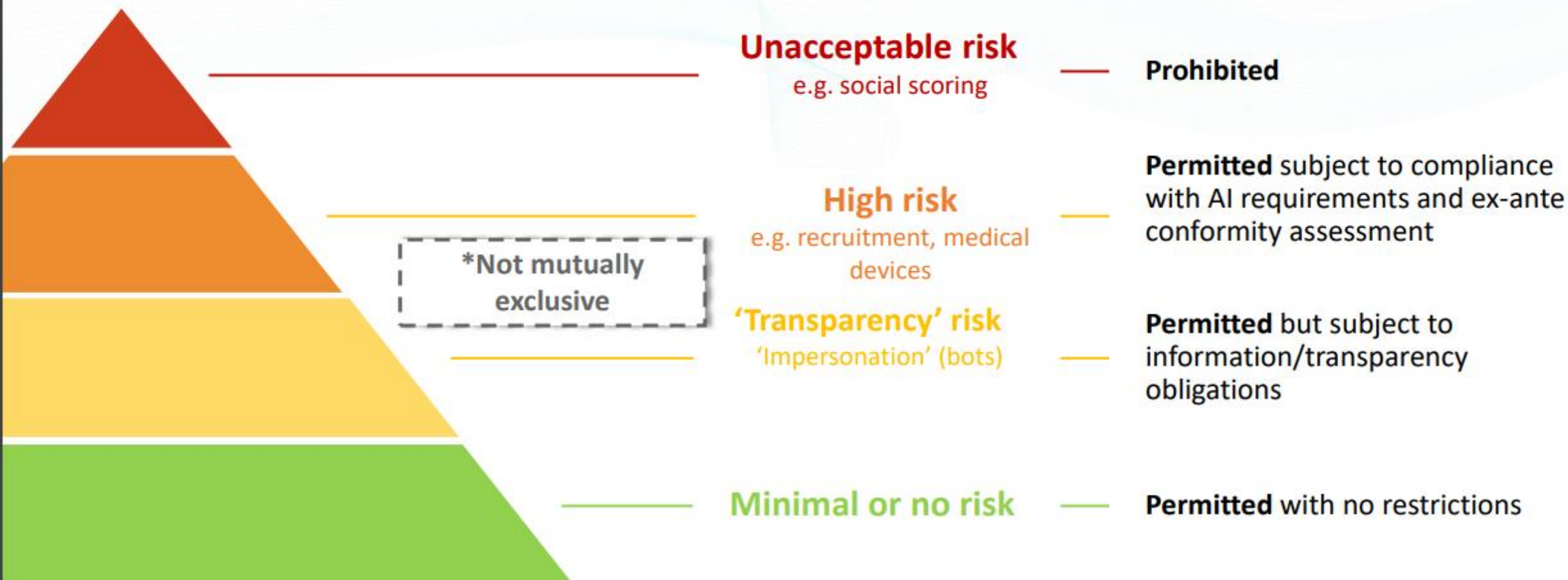
### *Common specifications*

1. **Where harmonised standards referred to in Article 40 do not exist** or where the Commission considers that the relevant harmonised standards are **insufficient** or that there is a need to address specific safety or fundamental right concerns, **the Commission may**, by means of implementing acts, **adopt common specifications** in respect of the requirements set out in Chapter 2 of this Title. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

2. The Commission, when preparing the common specifications referred to in paragraph 1,  gather the views of relevant bodies or expert groups established under relevant sectorial Union law.



## 2.1. Proposal for the Artificial Intelligence Act (7) Risk-based approach: an overview



*[Note: this slide is not part of AIA but taken from a presentation of the European Commission]*



## Article 5

1. The following artificial intelligence practices shall be prohibited:
  - (a) the placing on the market, putting into service or use of an AI system that deploys **subliminal techniques** beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person **physical or psychological harm**;
  - (b) the placing on the market, putting into service or use of an AI system that exploits any of the **vulnerabilities** of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;

## Article 5

1. The following artificial intelligence practices shall be prohibited:

(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for **the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour** or known or predicted personal or personality characteristics, with the **social score leading to** either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

# Prohibited AI Practices – ‘Real-time’ remote biometric identification systems ...

## Article 5

1. The following artificial intelligence practices shall be prohibited:

(d) the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

- (i) the targeted search for specific potential victims of crime, including missing children;
- (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
- (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State. Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).