



European
Commission

SHAPING EUROPE'S DIGITAL FUTURE

Introduction to the Artificial Intelligence Act proposal

Gabriele Mazzini

DG CNECT, European Commission

Intelligenza artificiale: definizioni, etica, strategia, prospettive, FAST

4 luglio 2023



Context & background

Package on AI April 2021

- **Communication:** “*Fostering a European approach to AI*”
- **Coordinated Plan** on AI 2021 review
- **Proposal for Artificial Intelligence Act**

Ecosystem of excellence

- R&D&I
- Testing and experimentation facilities
- Digital Innovation Hubs
- Skills and talent

through

- European programmes and national activities
- Creation of synergies in the Coordinated Plan on AI

Ecosystem of trust

- New regulatory proposal

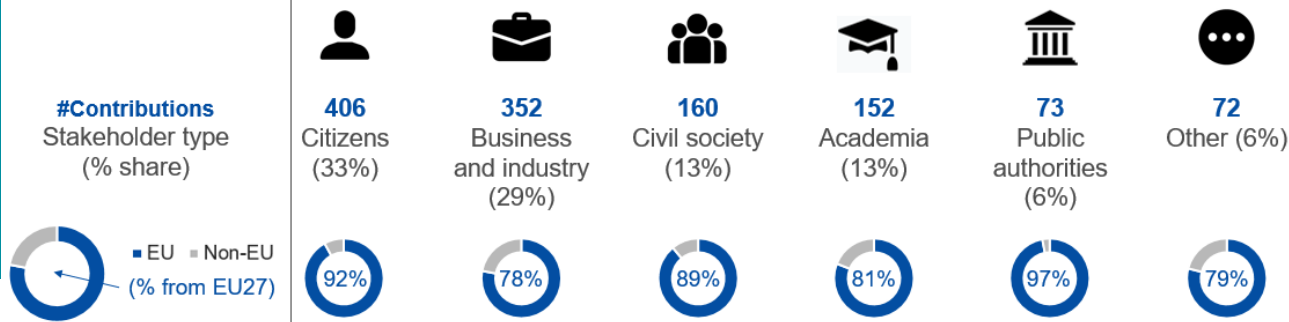
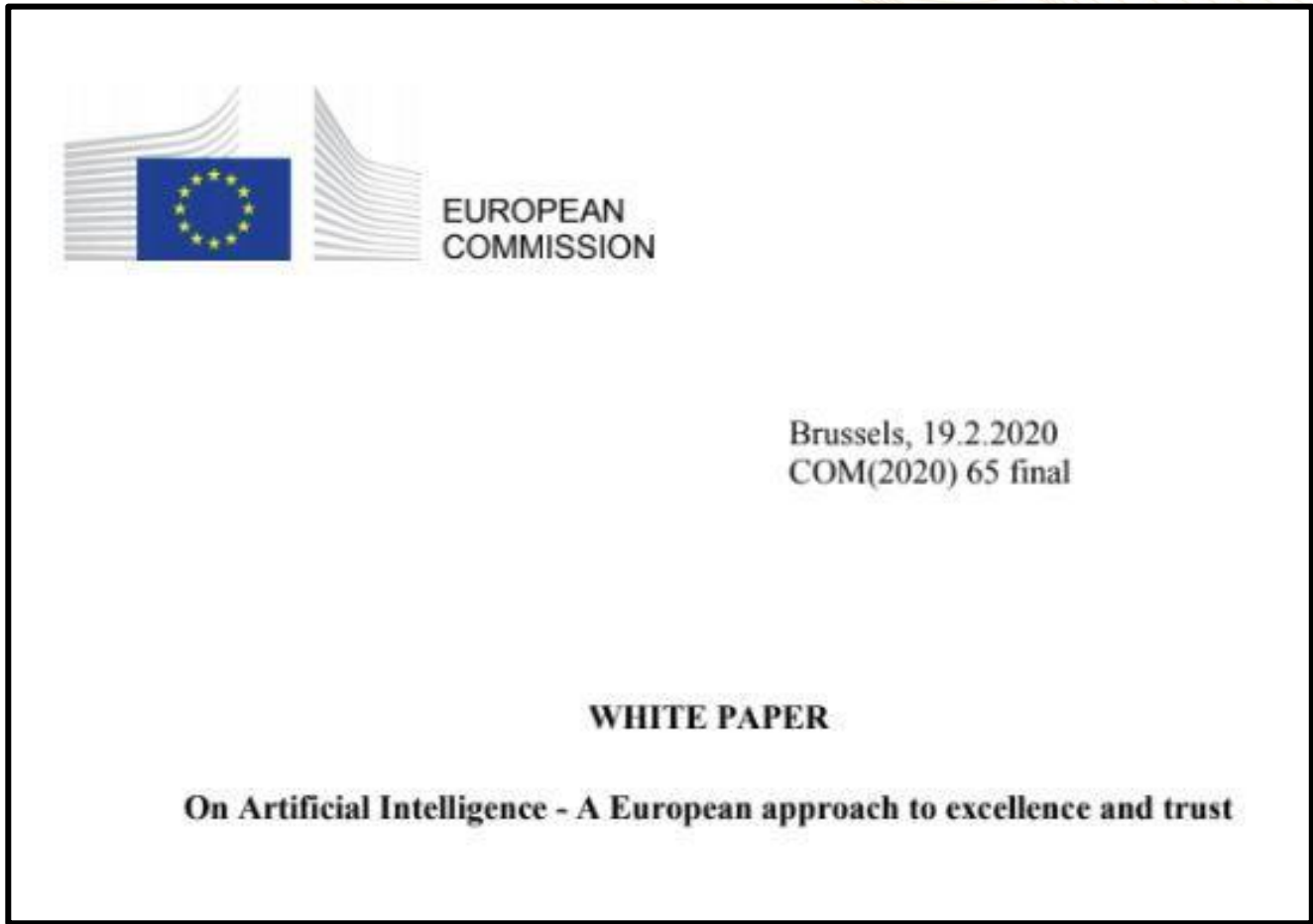
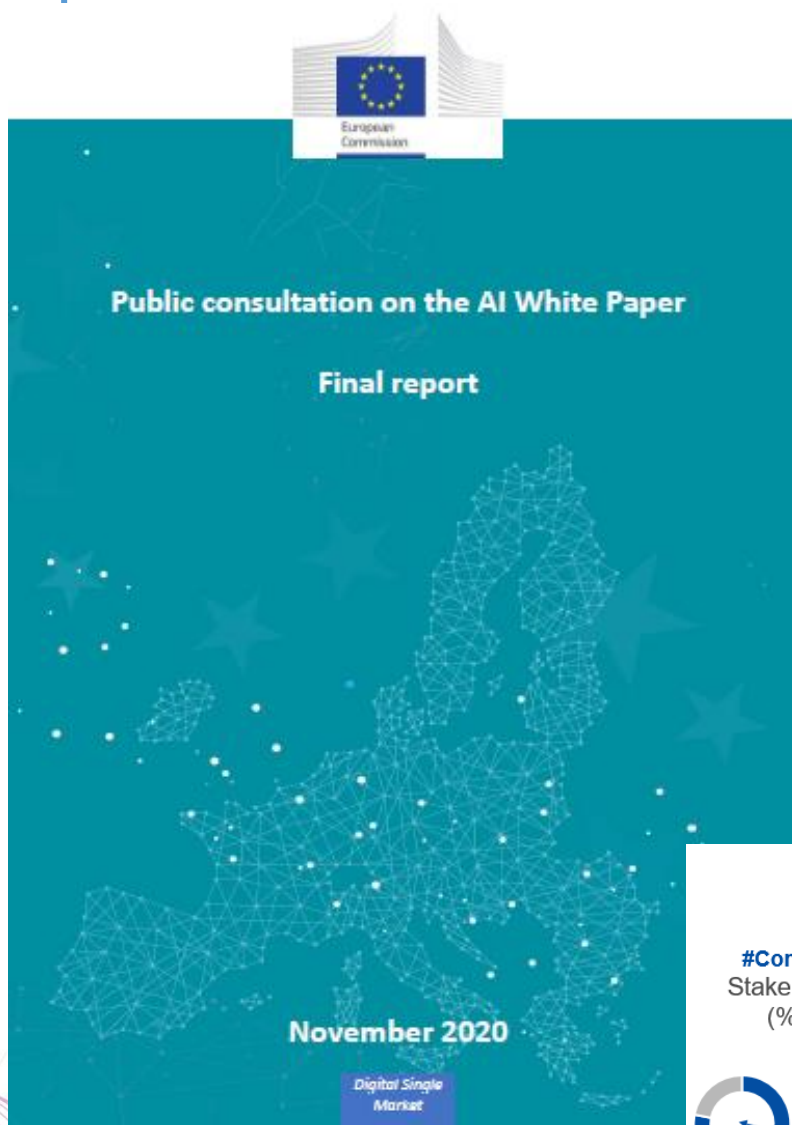
“..artificial intelligence will open up new worlds for us. But this world also needs rules.”



Background -2018-2019



Background - 2020



AI brings benefits to consumers, business and the society, but creates risks

Public consultation

Risks to fundamental rights

- ▶ 90% of respondents to the public consultation worry about AI breaching fundamental rights (ex. biometric identification)
- ▶ 87% about discriminatory outcomes

Risks to safety

- ▶ 82% of respondents to the public consultation are concerned that AI endangers safety (ex. AI in medical devices)

AI REGULATION

- ▶ 75% said that there is a need for new legislation or that current legislation may have gaps



The proposal for AI Act

Key regulatory concepts

Internal market legislation (mainly based on Art. 114 TFEU)

- ▶ “Classic” internal market rules for the **placing on the market and putting into service of AI systems**
- ▶ Aligned to vast EU acquis on product safety which shall be jointly applied (e.g. AI embedded in products)

Layered risk-based approach



- ▶ No regulation of the technology as such, but of **concrete use cases**
- ▶ Covers **risks to health, safety and fundamental rights**

Level playing field for EU and non-EU players

- ▶ Independent of origin of producer or user

Definition of AI

*“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**”*

(Art. 3(1) AI Act)

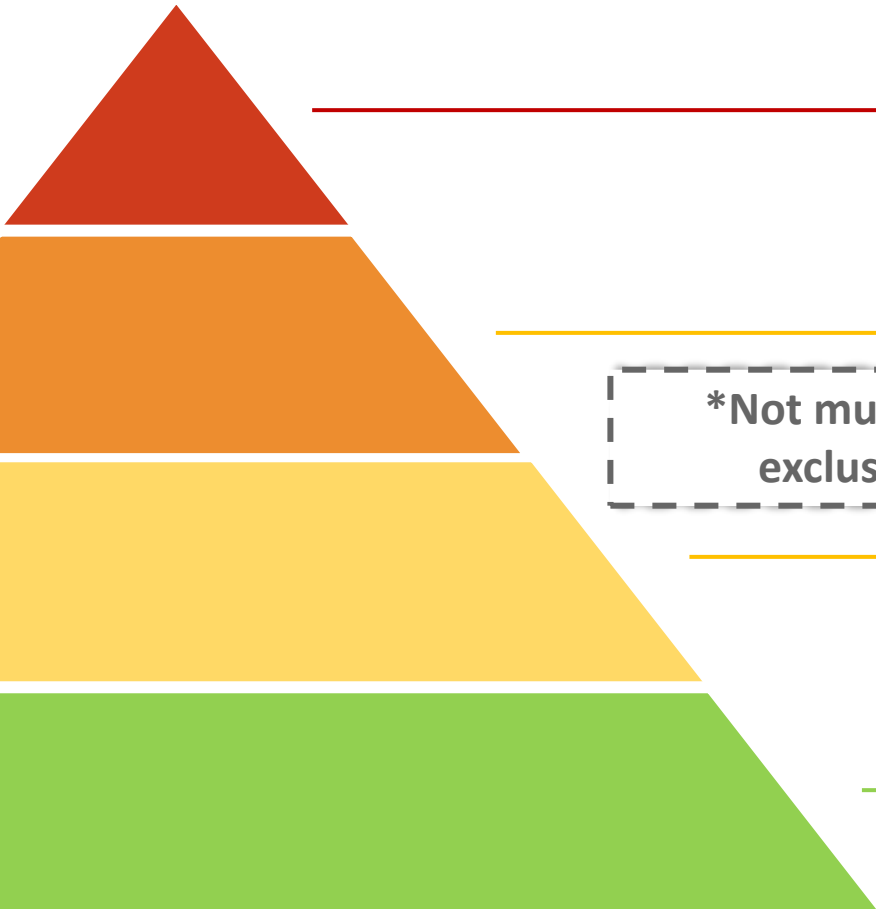
“a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments”

(OECD Council Recommendation on Artificial Intelligence, May 2019)

Risk-based approach

The higher the risk the stricter the rules

No regulation of the technology as such



***Not mutually exclusive**

Unacceptable risk

e.g. social scoring

Prohibited

High risk

e.g. recruitment, medical devices

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

'Transparency' risk

'Impersonation' (bots), deep fake

Permitted but subject to information/transparency obligations

Minimal or no risk

Permitted with no restrictions

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



X

Subliminal manipulation
resulting in physical/
psychological harm

X

Exploitation of vulnerabilities
resulting in physical/psychological harm

X

'Social scoring' by public authorities

X

'Real-time' remote biometric identification for law enforcement purposes in publicly accessible spaces
(with exceptions)

Remote biometric identification (RBI)

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

UNACCEPTABLE RISK



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)

HIGH RISK



➤ **Ex ante third party conformity assessment**

- Enhanced logging requirements
- “Four eyes” principle

High-risk Artificial Intelligence Systems (Title III, Chapter 1 & Annexes II and III)

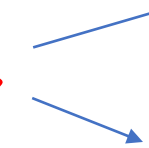


1 SAFETY COMPONENTS OF REGULATED PRODUCTS

(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation



New Legislative Framework - Section A



'Old Approach' - Section B

2 CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING AREAS

- ✓ 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



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



Establish and
implement **risk
management
system**
&
in light of the
**intended
purpose** of the
AI system

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

Draw up **technical documentation** & set up **logging capabilities** (traceability & auditability)

Ensure appropriate degree of **transparency** and provide users with **information** on capabilities and limitations of the system & how to use it

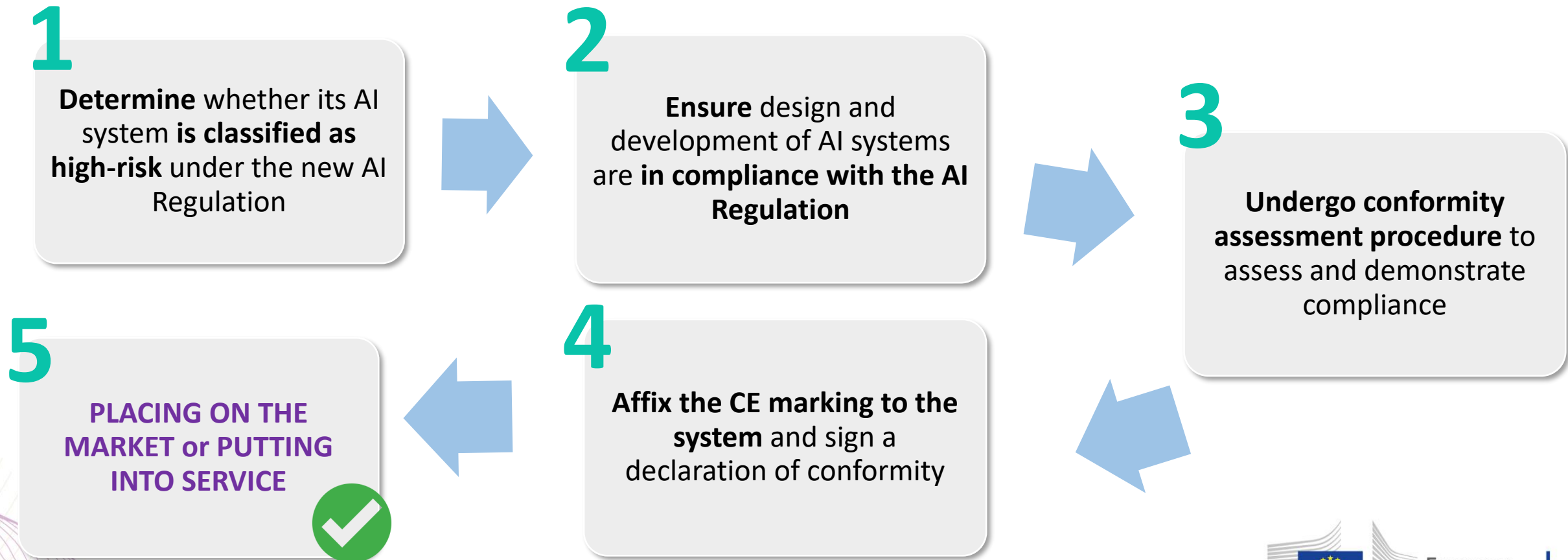
Ensure **human oversight** (measures built into the system and/or to be implemented by users)

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

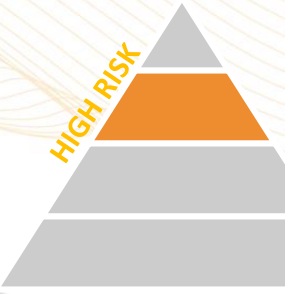
CE marking and process (Title III, chapter 4, art. 49.)

CE marking = indication that product complies with requirements of applicable Union legislation

In order to affix a CE marking, provider shall undertake **the following steps**:



Overview: obligations of operators (Title III, Chapter 3)



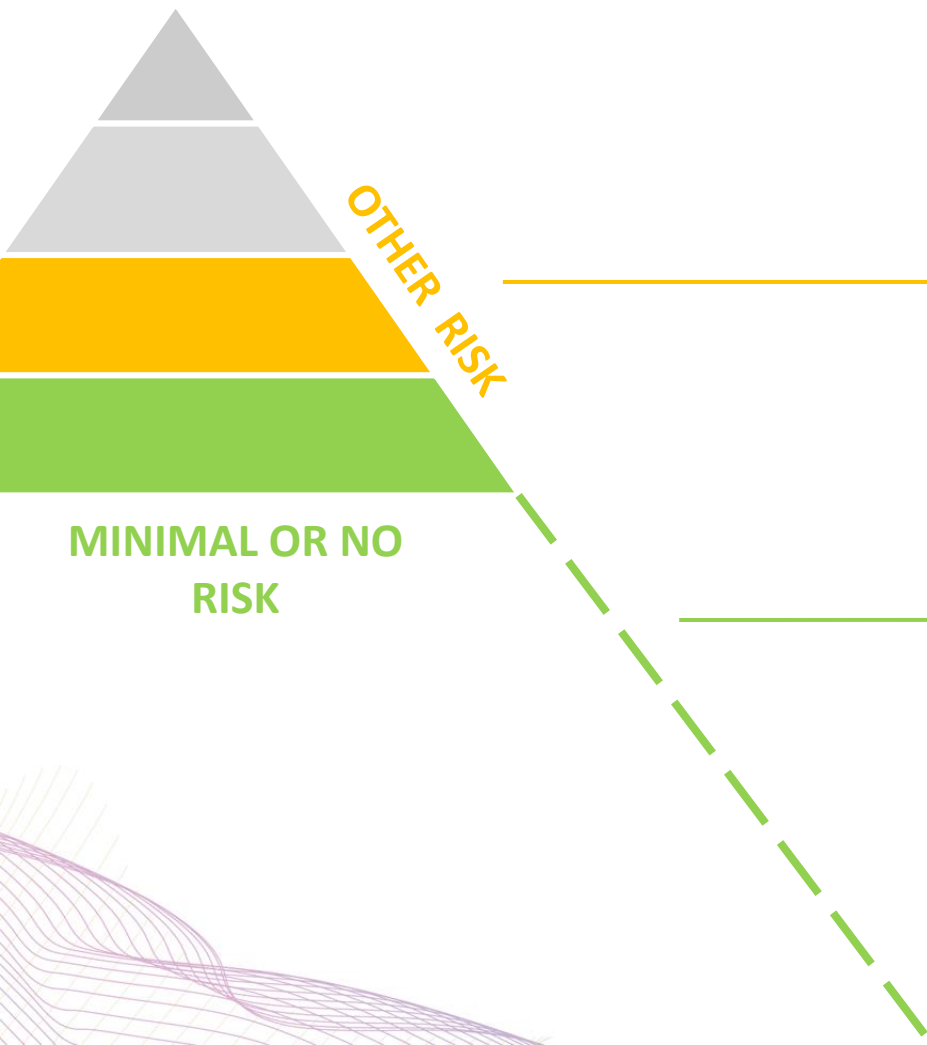
Provider obligations

- ▶ Establish and implement **quality management** system in its organisation
- ▶ **Register AI system** in EU database
- ▶ Conduct **post-market monitoring**
- ▶ **Collaborate** with market surveillance authorities

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)

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



Transparency obligations for certain AI systems (Art. 52)

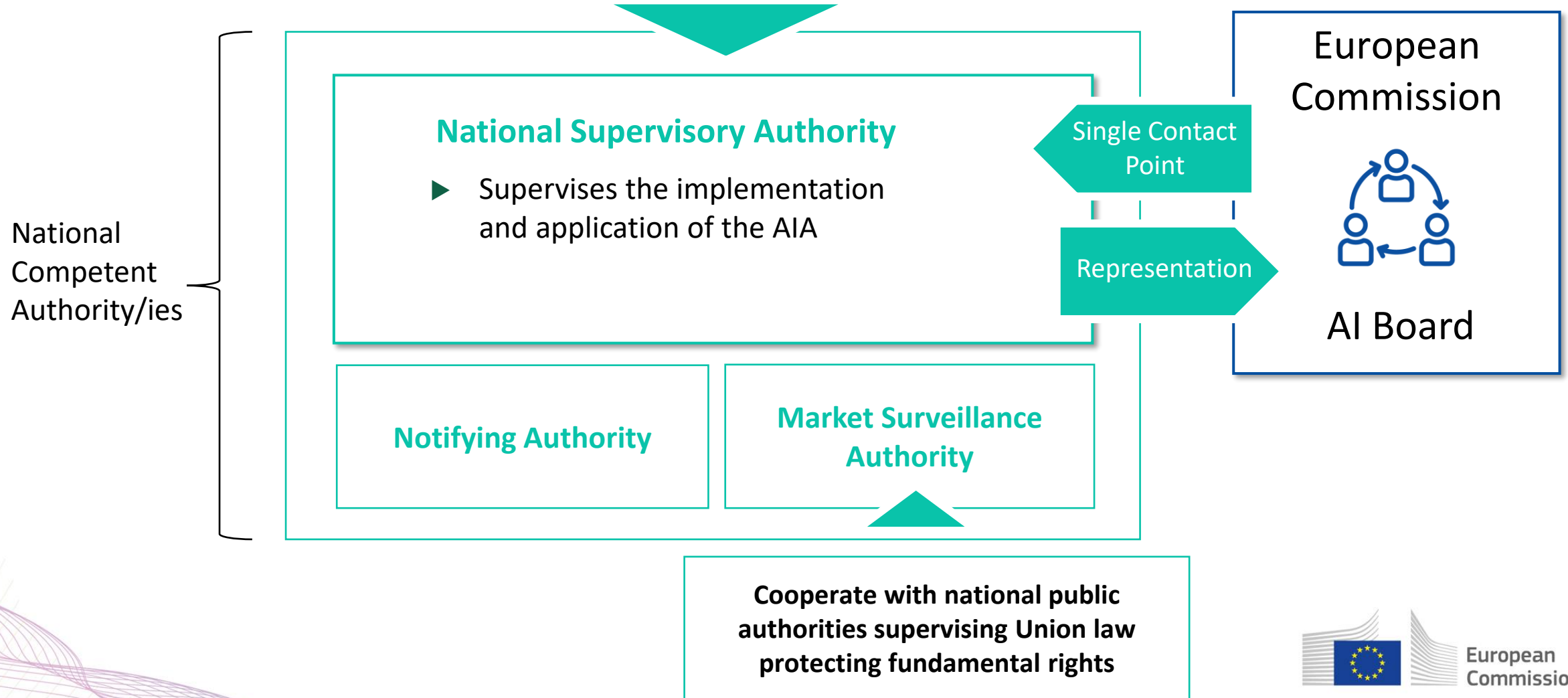
- ▶ **Notify humans** that they are **interacting with an AI system** unless this is evident
- ▶ **Notify humans** that they are **exposed to emotional recognition or biometric categorisation systems**
- ▶ Apply label to **deep fakes**

Possible voluntary codes of conduct (Art. 69)

- ▶ No mandatory obligations
- ▶ Commission and Board to encourage drawing up of codes of conduct (**voluntary application of requirements for high-risk AI systems or other requirements**)

Governance: national level

Member State designates

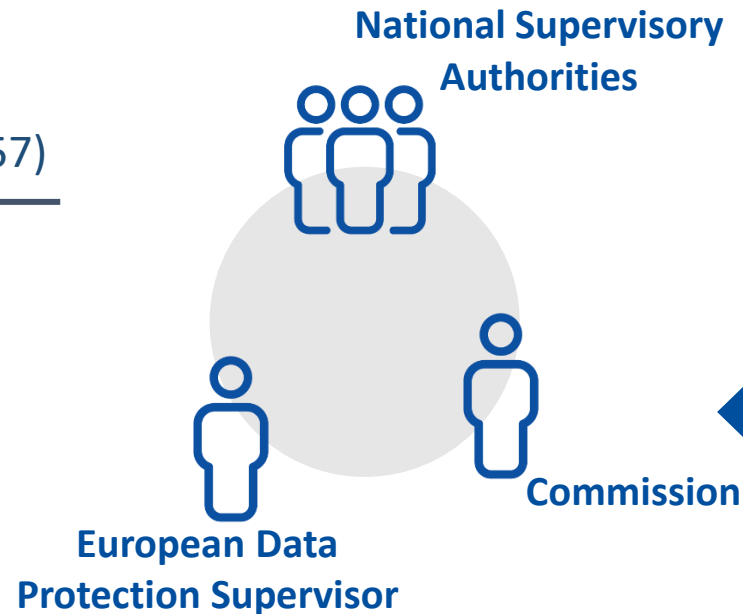


Governance: EU level

European AI Board

Structure and mandate (artt. 56 and 57)

- ▶ contribute to **effective cooperation** of national supervisory authorities and EC
- ▶ contribute to **guidance and analysis**
- ▶ assist in ensuring the **consistent application of the AI Regulation**



Other national authorities may be invited for issues of relevance for them

The Board may invite **external experts and observers**

European Commission
Secretariat of the Board

- ▶ Chair the Board
- ▶ Provide administrative and analytical support

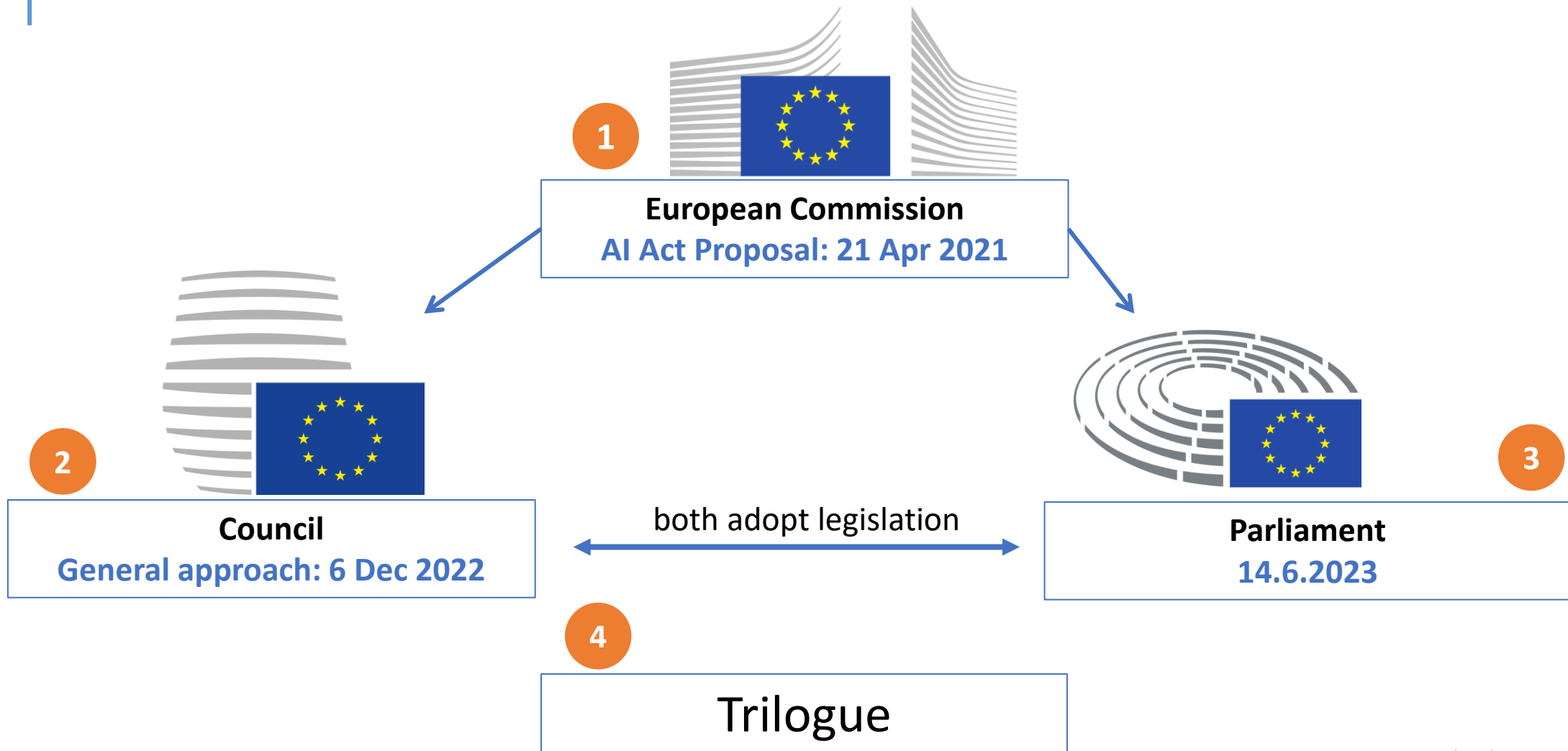
Subgroups

- ▶ for the purpose of examining specific questions



Next steps

Ordinary legislative procedure



State of play: ordinary legislative procedure

Parliament

- **Joint competence of IMCO & LIBE committees:** draft report from 20 April.
- In addition, five other committees have partial competence on different parts of the file: JURI & ITRE (exclusive), CULT (shared), ENVI & TRAN (opinion).

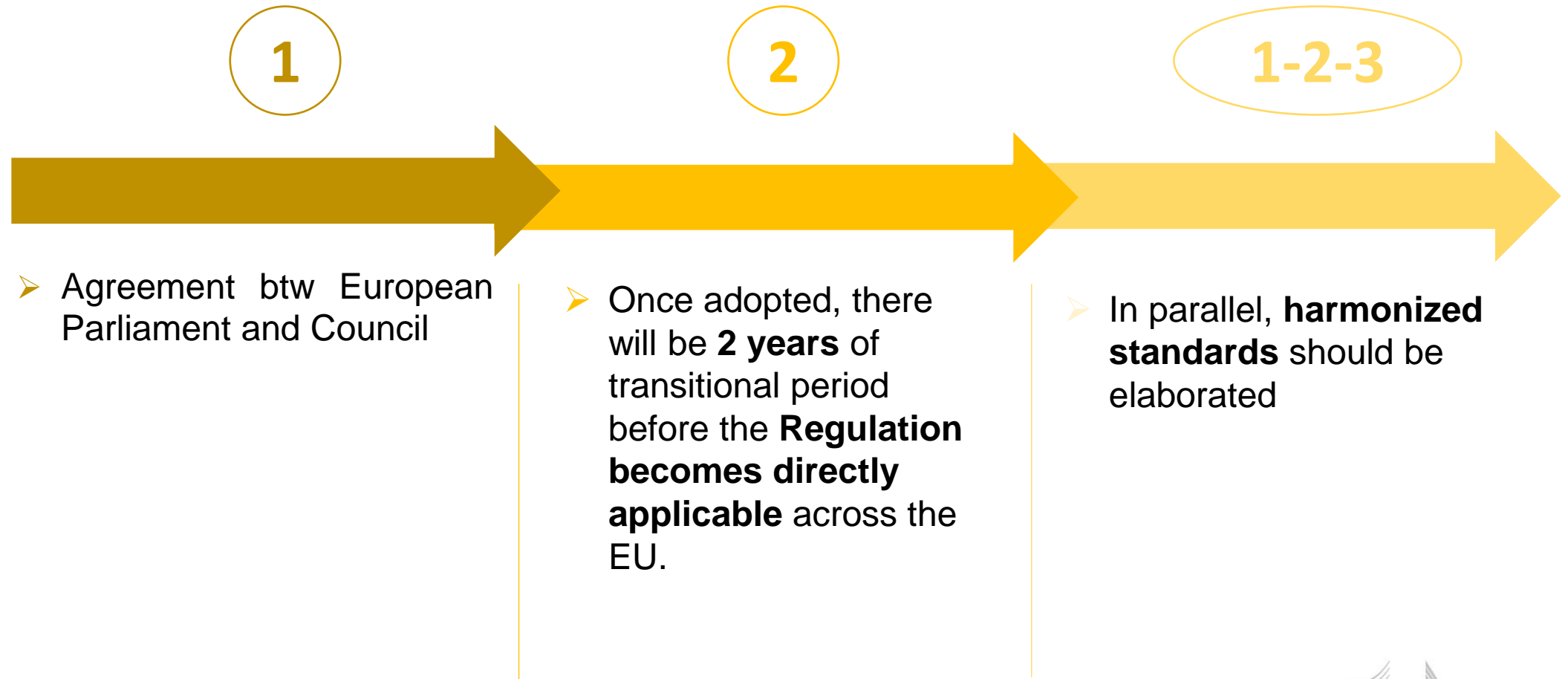
Council

- **PT Presidency**
- **SI Presidency**
- **FR Presidency** (full first reading)
- **CZ Presidency** (General Approach)

Some issues under discussion:

- **Definition of AI**
- **Prohibitions (notably biometrics)**
- **General-purpose AI systems**
- **List of high-risk AI systems**
- **Enforcement mechanism and governance**
 - AI Board and role of the Commission
- **Users obligations**

Timelines





Thank you

gabriele.mazzini@ec.europa.eu