European Commission

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

AI Package – April 2021

European Commission

AI package April 2021

A narrative that brings together the **proposal for a regulatory framework on AI and revised Coordinated Plan on AI**.

The AI package is a **key milestone on the way to achieving the EU ambition:**

Enable the EU to become **a world-class AI hub**, while ensuring that AI is **trustworthy**

BACKGROUND

- AI strategy *(4/2018)*
- Coordinated Plan on AI *(12/2018)*
- Human-centric AI Communication *(4/2019)*
  - AI HLEG Ethical Guidelines for Trustworthy AI
- White Paper on AI *(2/2020)*

Coordinated Plan on AI 2021 Review

European Commission

From intention to action: creating EU global leadership on trustworthy AI

Accelerate investments in AI technologies to drive resilient economic and social recovery

Private and public investments leveraging EU funding available through **Digital Europe** (DEP), **Horizon Europe** (HE) programmes and **Recovery and Resilience Facility (RRF)**.

Act on AI strategies and programmes by fully and timely implementing them to ensure that the EU fully benefits from the first-mover advantages;

A set of **specific actions** with a clearly indicated **timeline** and possible **cooperation and funding mechanisms.**

Align AI policy to remove fragmentation and address global challenges.

Between EU actions as well as between national and EU actions;

The 2020 **White Paper on AI**, the **European Green Deal** and the EU measures in response to the **Covid-19** pandemic;

National AI strategies

Building on learnings since 2018, two-step approach in each chapter

Review + Outlook

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 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 KEY SECTORS

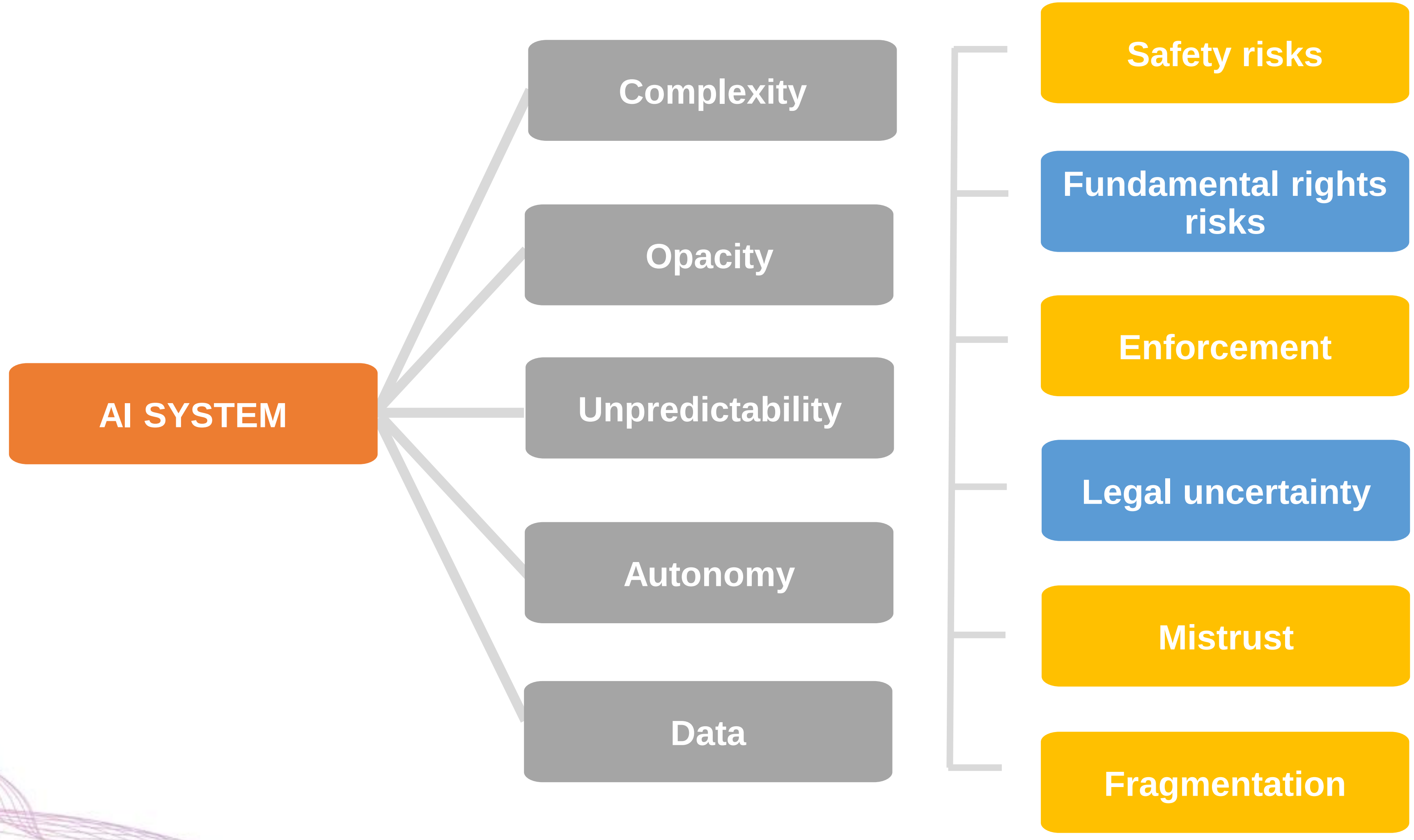
- Climate and environment
- Health
- Strategy for Robotics in the world of AI
- Public sector
- Law enforcement, immigration and asylum
- Mobility
- Agriculture

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

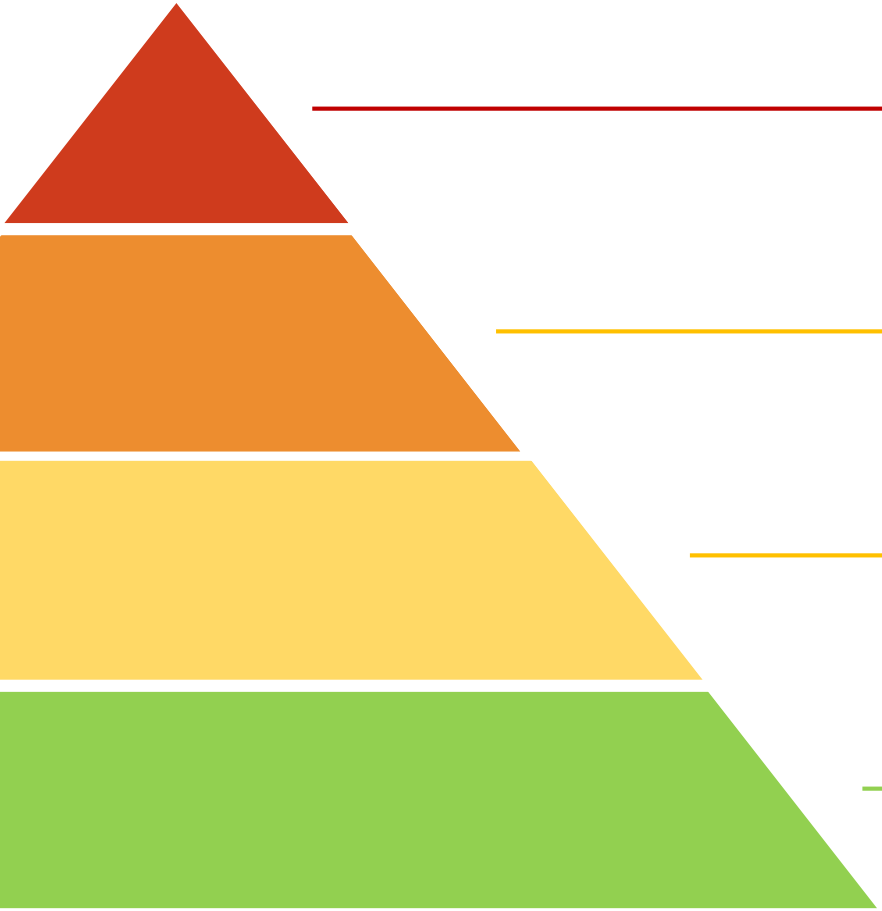
Proposal for a legal framework on AI

European
Commission

Why do we regulate AI use cases?

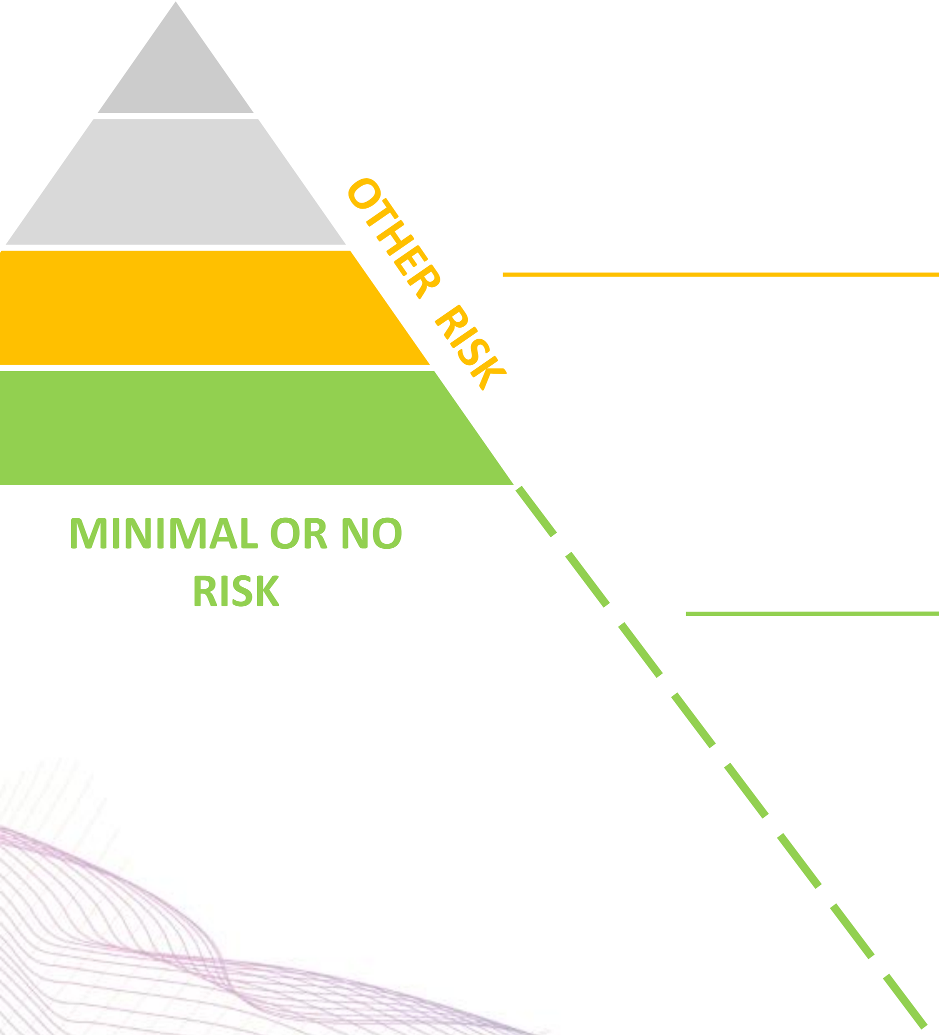


A risk-based approach to regulation



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
AI with specific transparency obligations Impersonation (bots)	**Permitted** but subject to information/transparency obligations
Minimal or no risk	**Permitted** with no restrictions

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



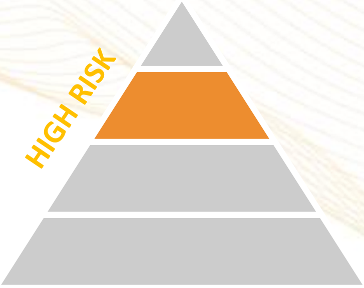
New transparency obligations for certain AI systems (Art. 52)

- **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**

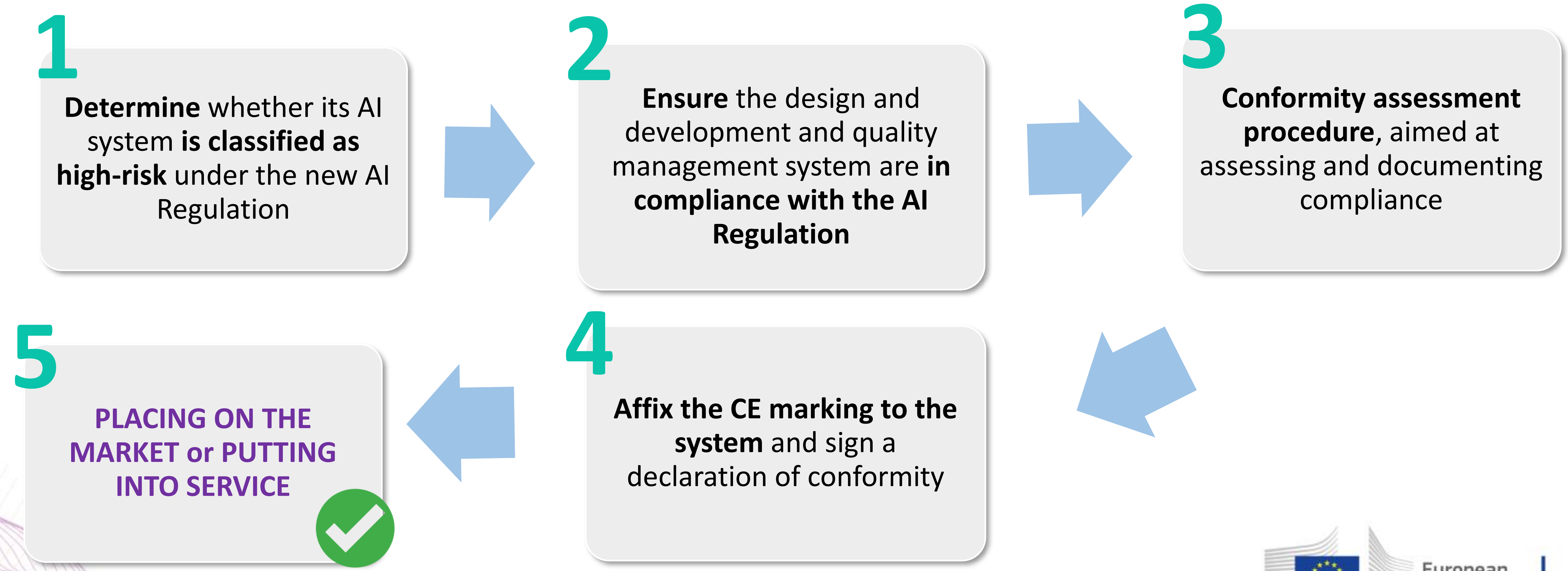
(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation

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 relevant Union legislation regulating the product in question. In order to affix a CE marking to a high-risk AI system, a provider is undertake **the following steps:**



1 **Determine** whether its AI system **is classified as high-risk** under the new AI Regulation

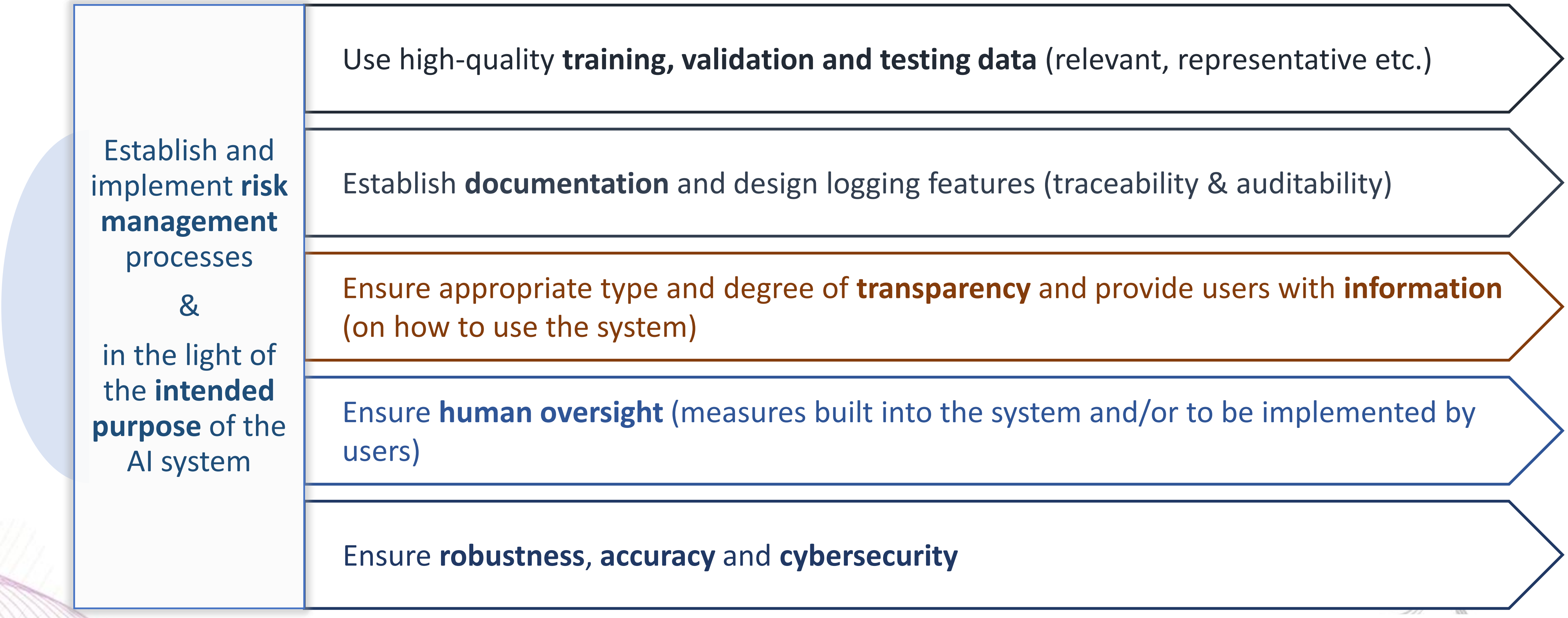
2 **Ensure** the design and development and quality management system are **in compliance with the AI Regulation**

3 **Conformity assessment procedure**, aimed at assessing and documenting compliance

4 **Affix the CE marking to the system** and sign a declaration of conformity

5 **PLACING ON THE MARKET or PUTTING INTO SERVICE**

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



Establish and implement **risk management** processes

&

in the 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 type and 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 III, Chapter 3)

Provider obligations

- Establish and implement a **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** and potentially re-assessment of the system (in the event of significant modifications)
- Register AI system in EU database
- Affix CE marking and sign declaration of conformity
- 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)

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

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 reporting 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 the event 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 conflicts with EU values is prohibited (Title II, Article 5)

✗ **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.

✗ **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.

✗ **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.

✗ **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.

Thank you