



SHAPING EUROPE'S DIGITAL FUTURE

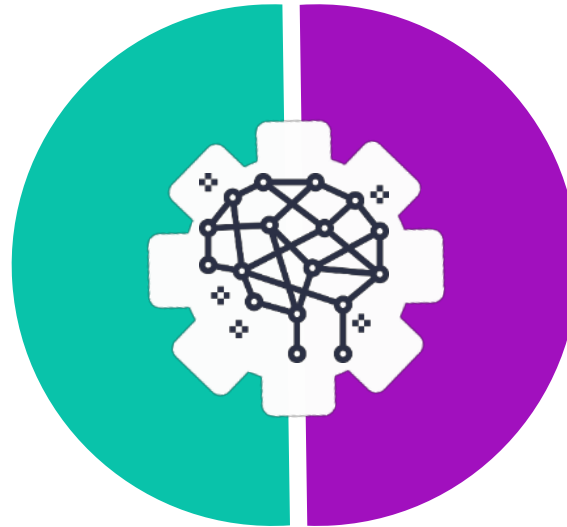
EU approach to Artificial Intelligence and the world of labour

Yordanka Ivanova
Legal and policy officer
DG CNECT, European Commission

The baseline

AI is good ...

- For citizens
- For business
- For the public interest



... but may create some risks

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

European AI policy (2018-2021)

Key initiatives:

- **European Strategy on AI** (April 2018)
- **Guidelines for Trustworthy AI** developed in 2019 by the High-Level Expert Group on Artificial Intelligence (HLEG)
- First **Coordinated Plan on AI** (December 2018)
- The Commission's **White Paper on AI** (February 2020) followed by a **public consultation**.
- **AI package** (April 2021)
 - Coordinated plan on AI (review)
 - Proposal for an AI Regulation

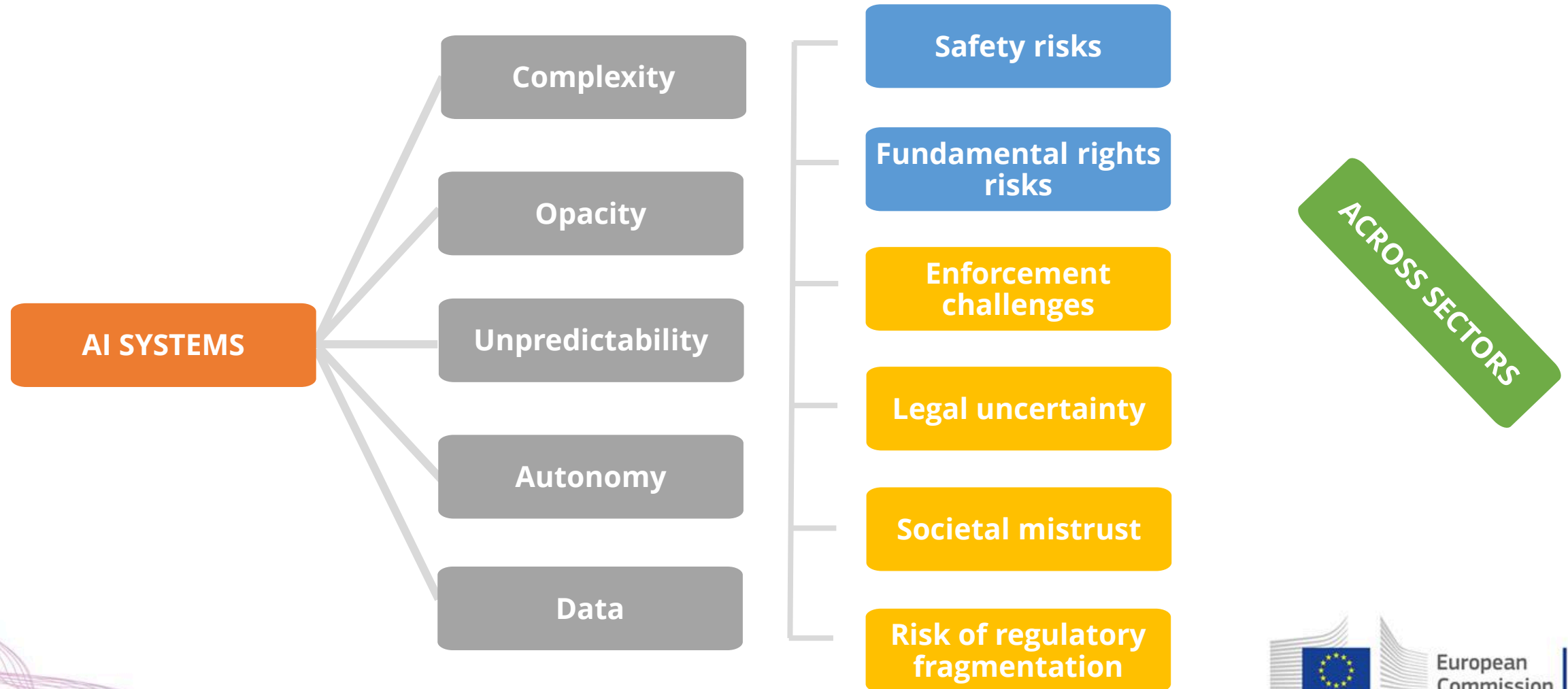


Updated Coordinated Plan on AI (review from 2018): joint commitment between the Commission and Member States



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

Why do we need an AI regulation in Europe?



Proposal for a Regulation on AI

Horizontal legislation laying down uniform rules for AI in the EU market

- ▶ “Classic” internal market rules applicable to the **placing on the market, putting into service and use of AI systems**
- ▶ Two main objectives:
 - ▶ **create a single market for trustworthy AI in EU**
 - ▶ **address risks to safety and fundamental rights**
- ▶ Consistent with and complementing existing EU and national law (e.g. employment, data protection)

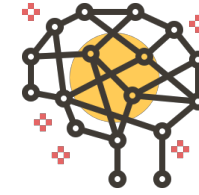
Innovation-friendly and risk-based legislation

- ▶ Provide **legal certainty** to operators and stimulate **trust** in the market
- ▶ No overregulation: designed to intervene only where strictly needed following a risk-based approach

Creates a level playing field for EU and non-EU players

- ▶ Applicable independent of origin of producer or user

Definition of Artificial Intelligence



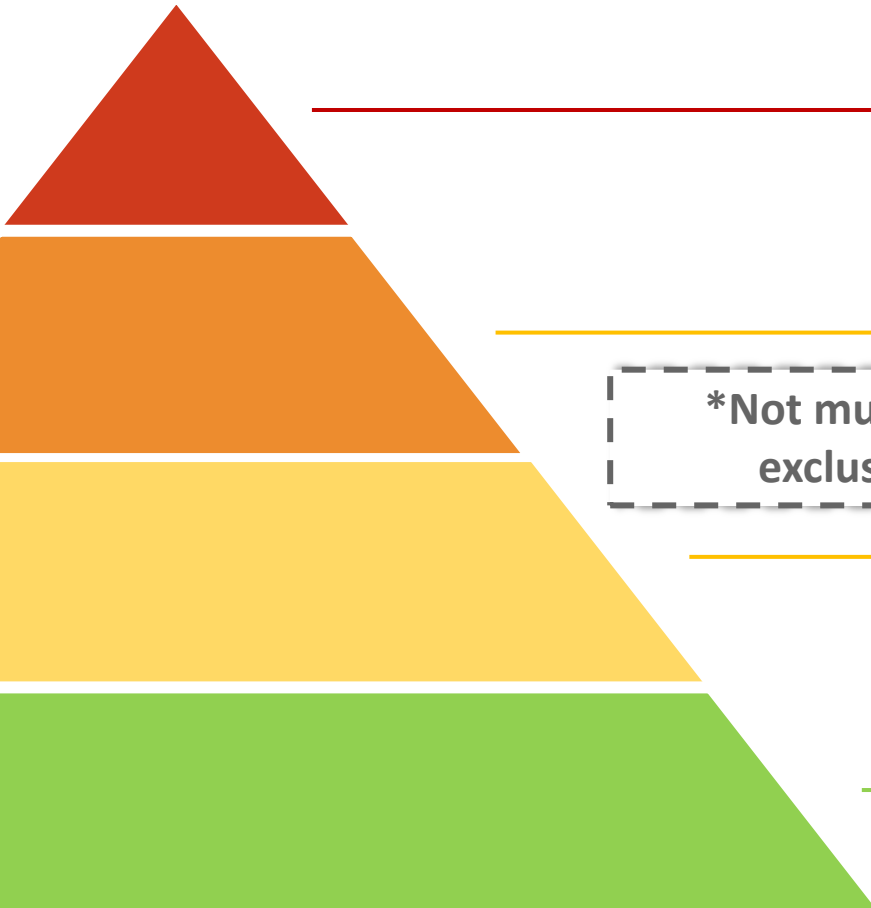
“a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with”

- ▶ 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)

Risk-based approach

The higher the risk the stricter the rules

No regulation of the technology as such



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

***Not mutually exclusive**

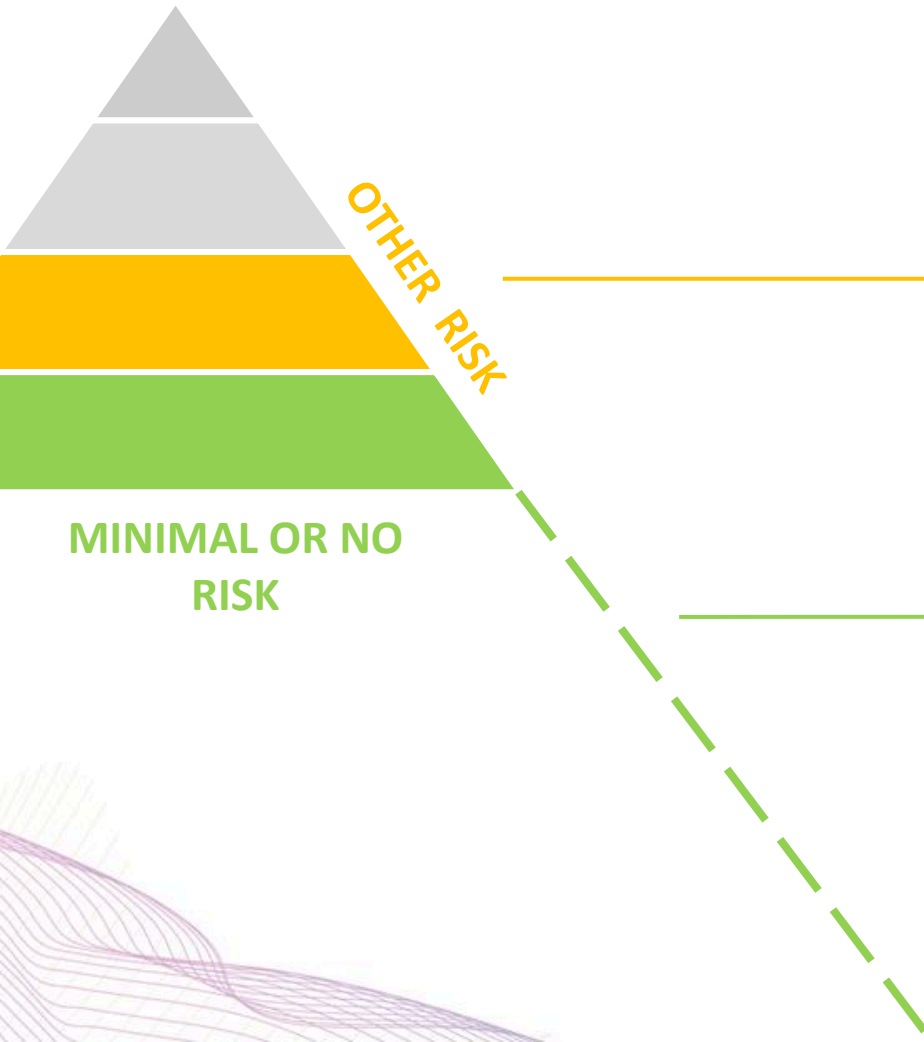
'Transparency' risk
'Impersonation' (bots)

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)



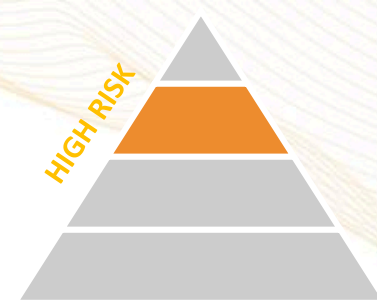
Transparency obligations for certain AI systems (Art. 52)

- ▶ **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**)

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



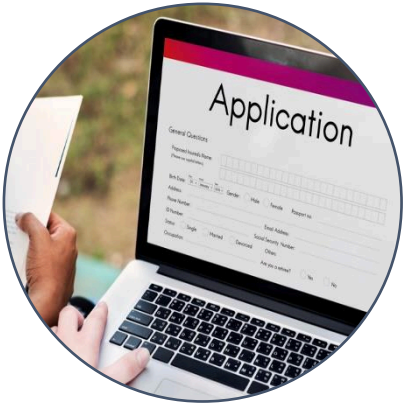
1 SAFETY COMPONENTS OF REGULATED PRODUCTS

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

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

Employment, workers management and access to self-employment



AI systems intended to be used for **recruitment or selection of natural persons**, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;



AI intended to be used for **making decisions on promotion and termination** of work-related contractual relationships, for **task allocation** and for **monitoring and evaluating performance and behavior** of persons in such relationships

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

HIGH RISK

Establish and implement **risk management** processes

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

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

➤ for RBI applications - enhanced logging requirements

Ensure appropriate degree of **transparency** and provide users with **information** (on how to use the system, its capabilities and limitations)

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

➤ Enhanced oversight for RBI applications - “Four eyes” principle

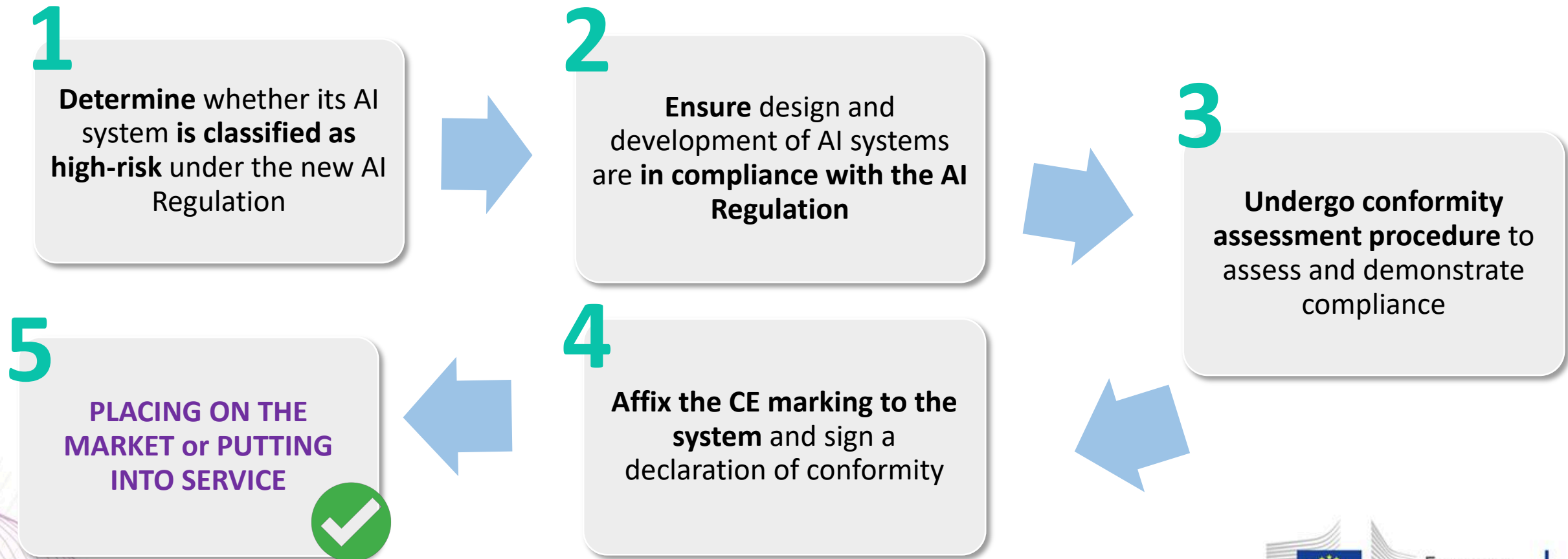
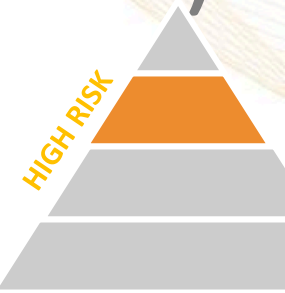
Ensure **robustness, accuracy** and **cybersecurity**

NB! Harmonised technical standards developed by ESOs will support providers to demonstrate compliance

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**:



Obligations of operators (Title III, Chapter 3)

HIGH RISK

Provider obligations (incl. companies developing in-house)

- ▶ Undergo **conformity** and potentially re-assessment of the system (in case of significant modifications) to demonstrate compliance with AI requirements
- ▶ Establish and Implement **quality management** system in its organisation
- ▶ Draw-up and keep up-to-date **technical documentation**
- ▶ **Keep logs** to monitor the operation of the high-risk AI system (when empowered by law or the user)
- ▶ **Register** stand-alone AI system in public EU database
- ▶ **Affix CE** marking and sign declaration of conformity
- ▶ Conduct **post-market monitoring** and take corrective action
- ▶ **Report serious incidents and malfunction** that can pose risks to fundamental rights
- ▶ **Collaborate** with market surveillance authorities

User obligations (AI developed in-house or bought off the shelf)

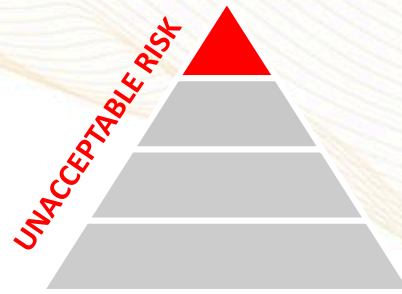
- ▶ Ensure **human oversight** and operate AI system in accordance with the **instructions of use**
- ▶ **Monitor** operation for possible risks
- ▶ **Inform the provider or distributor about any serious incident** or any malfunctioning
- ▶ Use the information given by the provider for the **data protection impact assessment** (where applicable)



Existing legal obligations for users continue to apply (e.g. under employment law

see also recital 31)

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



'Social scoring' by public
authorities

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.



**'Real-time' 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.

Supporting innovation (Title V)

**Regulatory
sandboxes
Art. 53 and 54**

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



Governance and Enforcement (Title VIII and IX)

National level

Key role for enforcement

▶ National Market Surveillance Authorities



▶ Cooperation with other authorities responsible for enforcement of fundamental rights legislation

European level

Coordination of implementation and exchange

▶ European Artificial Intelligence Board



▶ Commission to act as Secretariat

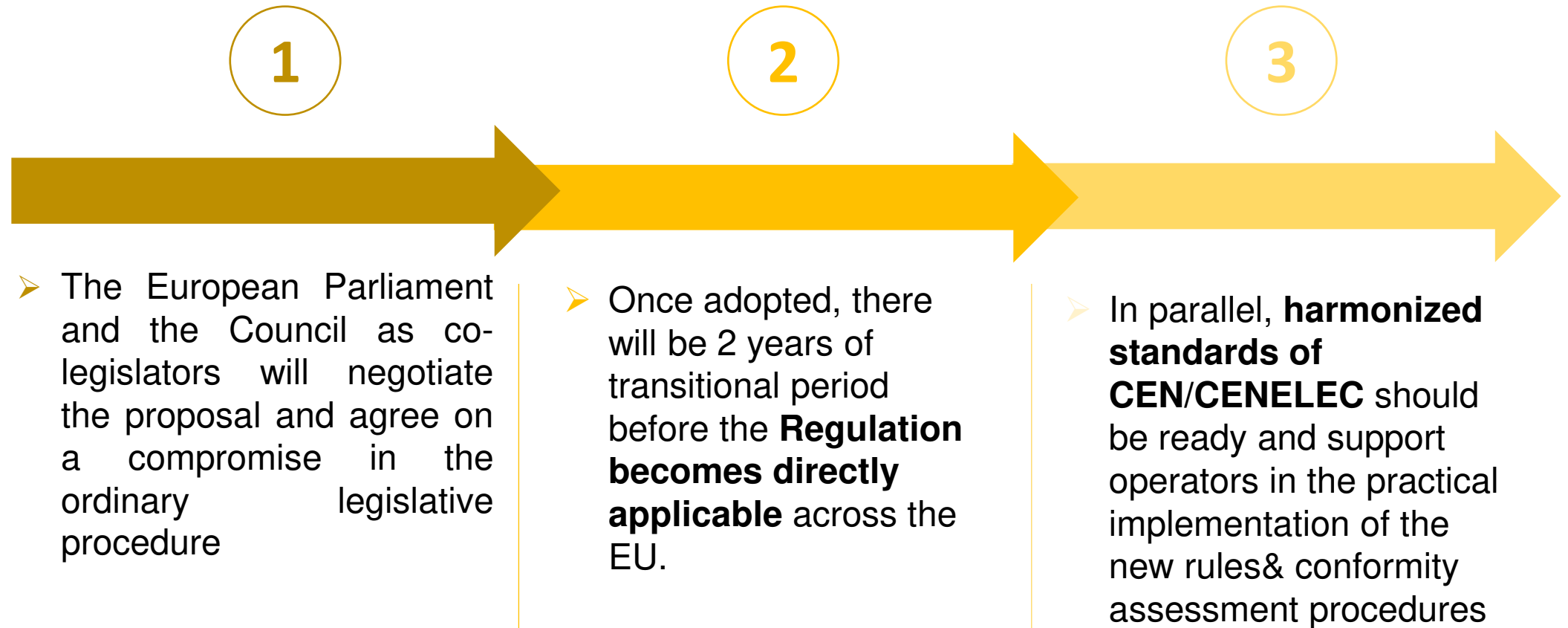


▶ Expert Group*

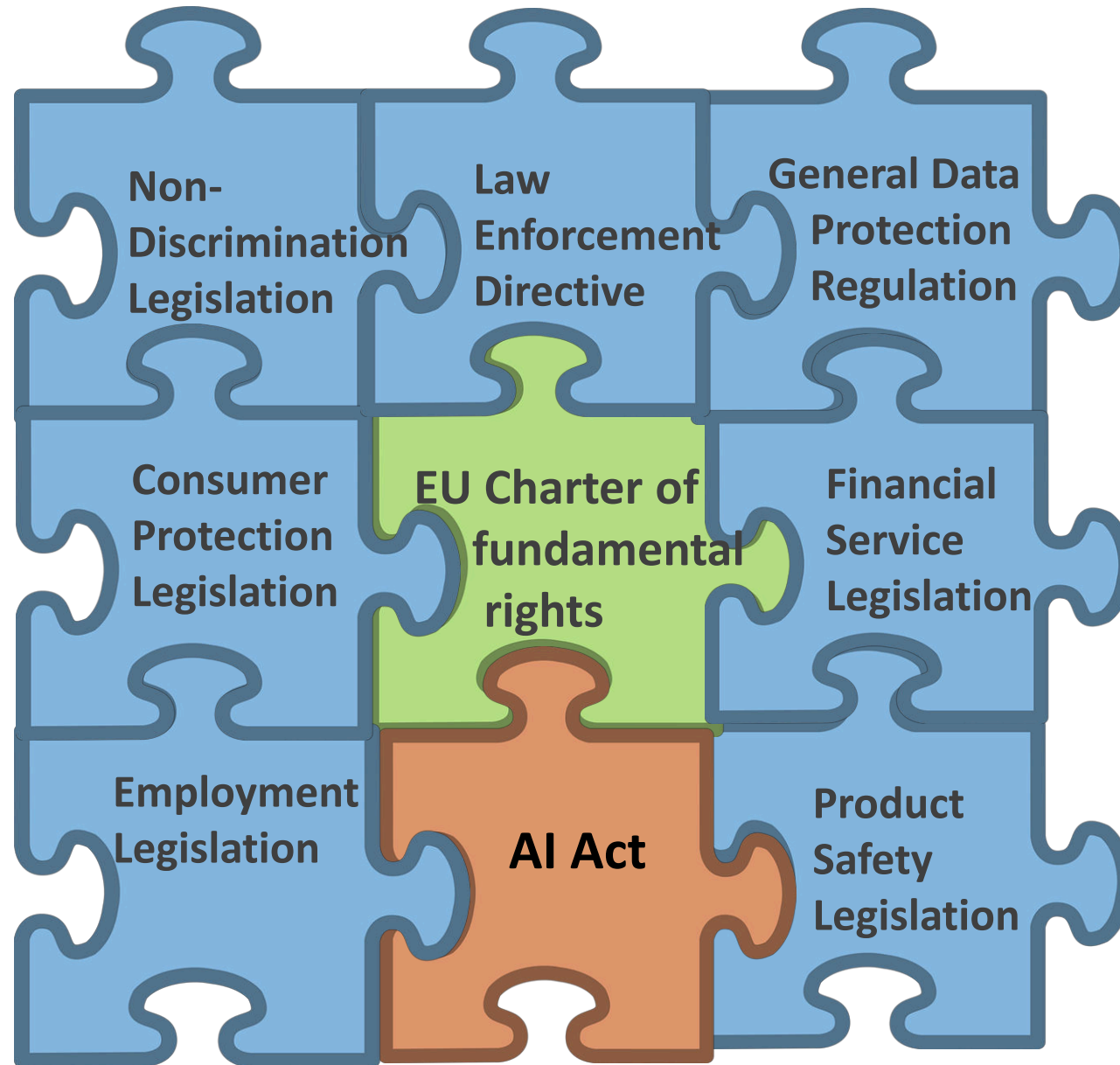


*Not foreseen in the regulation but the Commission intends to introduce it in the implementation process.

Next steps

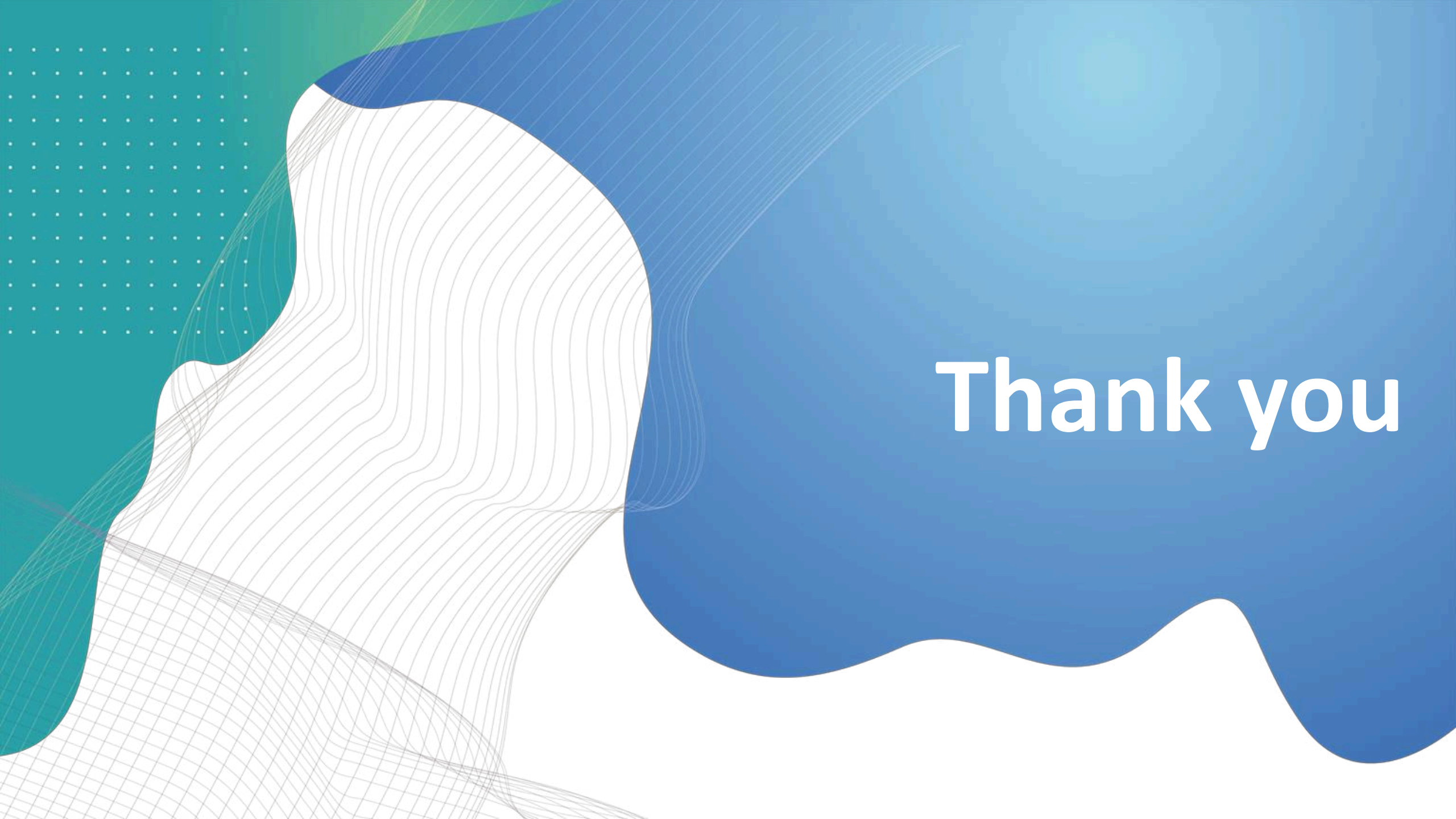


Comprehensive EU regulatory approach to AI



Making Europe fit for the digital age

- Proposal for AI Regulation
- Proposal for a Platform work Directive
- Digital decade: digital targets for 2030
- Data strategy, the Data Governance Act and proposal for a Data Act
- Proposals for Digital services Act and Digital Market Act (DSA and DMA)
- Proposal for review of the Network and Information Security Regulation (NIS2)
- Proposal for the eIDAS Regulation



Thank you