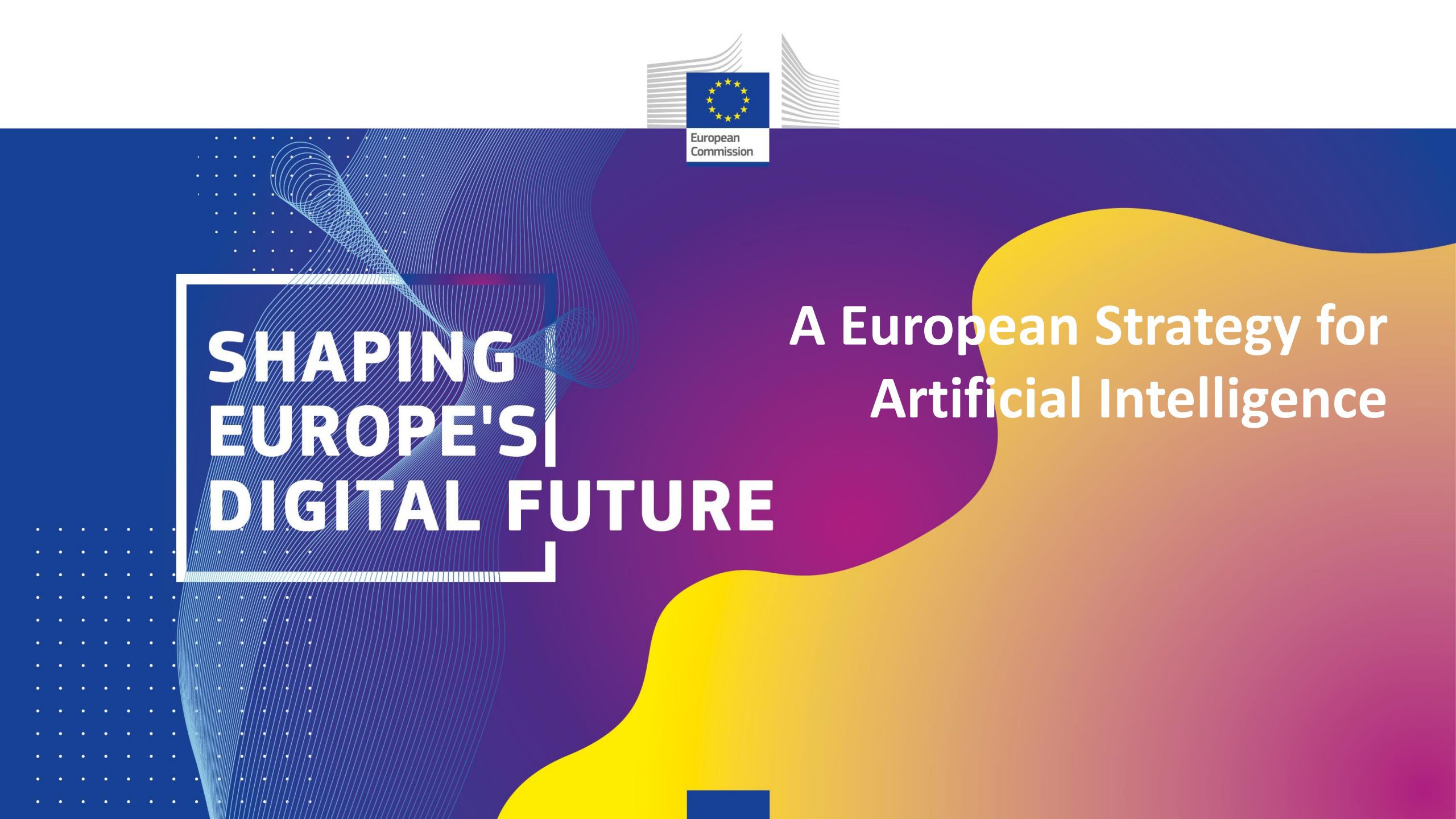

European Commission
SHAPING EUROPE'S DIGITAL FUTURE
A European Strategy for Artificial Intelligence

1. Proposal for a legal framework on AI

Why a Regulation on AI?

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

"Whether it's precision farming in agriculture, more accurate medical diagnosis or safe autonomous driving - artificial intelligence will open up new worlds for us. ***But this world also needs rules****."*

President Ursula von der Leyen, State of the Union 2020

European Commission

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)

Excluded: AI developed used exclusively for military purposes

Layered risk-based approach

- No regulation of the technology as such, but of concrete high-risk use cases
- Covers risks to health, safety and/or fundamental rights

Level playing field for EU and non-EU players

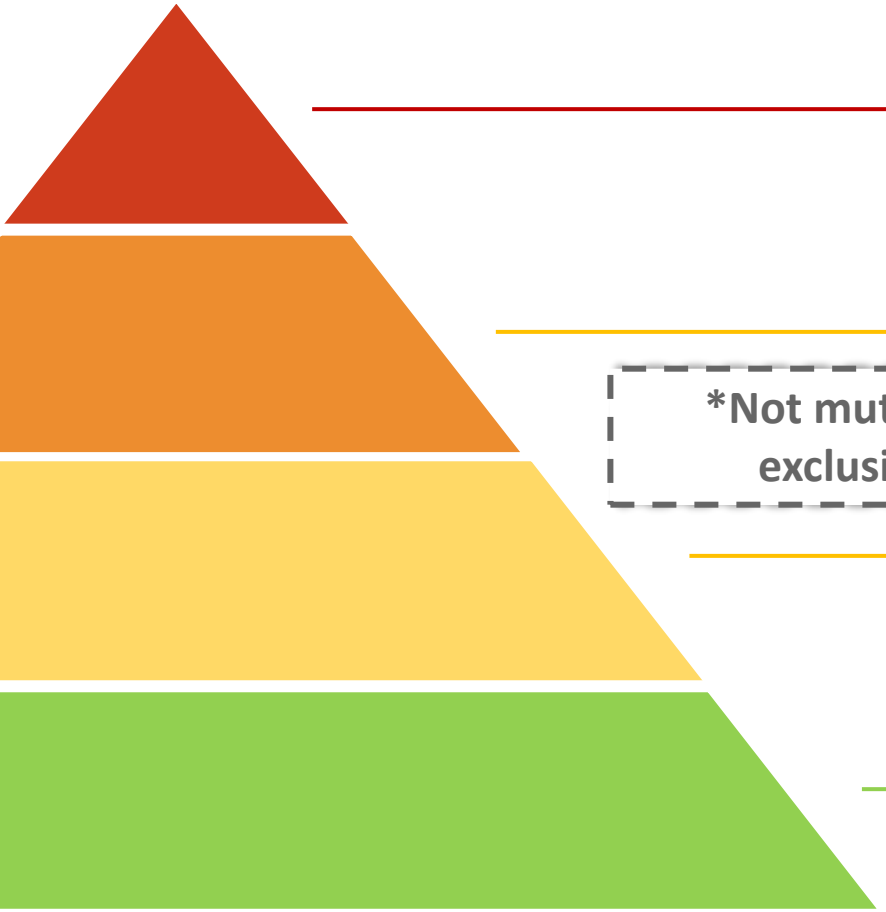
- Independent of origin of producer or user

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)

A risk-based approach



*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)

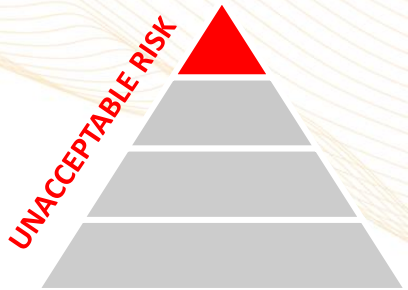
Permitted but subject to information/transparency obligations

Minimal or no risk

Permitted with no restrictions

European Commission

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.

European Commission

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

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

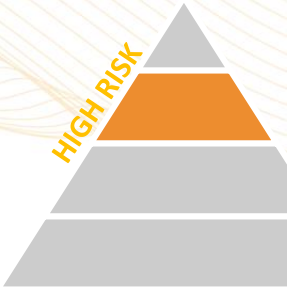
Establish and implement **risk management system**

&

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**

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



Provider obligations

- Establish and Implement **quality management** system in its organisation
- Draw-up and keep up to date **technical documentation**
- Undergo **conformity assessment** and potentially re-assessment of the system (in case of substantial modification)
- **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)

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:**

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

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

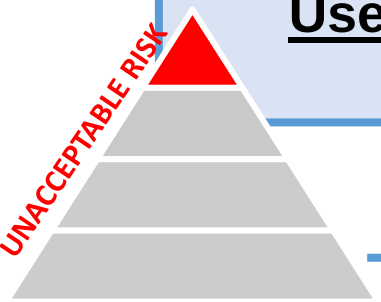
3 **Undergo conformity assessment procedure** to assess and demonstrate compliance

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

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

European Commission

Remote biometric identification (RBI)



Use of real-time RBI systems for law enforcement (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 ex-post)

- **Ex ante third party conformity assessment**
- Enhanced logging requirements
- "Four eyes" principle

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

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)**

European Commission

Supporting innovation (Title V)

Regulatory sandboxes
Art. 53 and 54

- ✓ **National authorities** in charge of individual schemes, cross-border sandboxes possible
- ✓ Uniform **common principles** and criteria
- ✓ **Cooperation** between MS and a future AI Board to ensure common European approach
- ✓ Further processing of personal data in the public interest in the sandboxes

Support for SMEs/start-ups
Art. 55

- ✓ **Priority access** to regulatory sandboxes for SMEs and start-ups
- ✓ **Support SMEs viability:** specific consideration of small-scale providers, with regard to certain obligations and conformity assessment fees.
- ✓ **Harmonised technical standards** to help small providers demonstrate compliance

The governance structure (Titles VI and VII)

European level

Artificial Intelligence Board

- National Supervisory Authorities
- EDPS
  - European Commission Secretariat

- Collect and **share best practices & expertise**
- contribute to uniform administrative practices in the MS
- Provide advice, opinions, recommendations on AI issues:
  - Standards (including harmonized standards) & technical specifications
  - Preparation of guidance documents

National level

National Competent Authorities, incl. National Supervisory Authority

- Responsible for the application and implementation of the Regulation
  - Oversight of conformity assessment bodies
  - Market surveillance activities ex Regulation (EU) 2019/1020

2. Coordinated Plan on AI 2021 Review

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

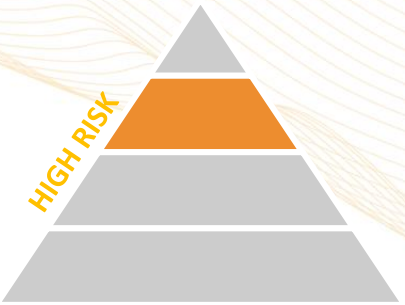
- Climate and environment
- Health
- Strategy for Robotics in the world of AI
- Public sector
- Law enforcement, immigration and asylum
- Mobility
- Agriculture

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

Thank you

Back up slides legal text

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 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.**

Classification of AI systems as high-risk (Title III, chapter 1 and Annex III)

Including available evidence

Risk assessment to determine likelihood and severity of harm to safety/fundamental rights based on the following criteria:

- Existing use of AI
- Previous harms or major concerns
- Potential impact & scale of a harm
- Dependency of affected person on outcome determined by AI system
- Reversibility of outcome produced by an AI system (e.g. physical harm)
- Availability/effectiveness of existing legal remedies

Biometric identification in a shopping mall

AI as safety component of a grid management system

AI to dispatch emergency medical aid

AI to filter resumes of applicants

AI to grade students

AI to evaluate creditworthiness

AI to process asylum applications*

...

Risks to health, safety and/or fund. rights in the following areas:

- Biometric identification and categorisation
- Management & operation of critical infrastructure & services
- Education & vocational training
- Employment & workers management
- Access to & enjoyment of private services & public services & benefits
- Law enforcement
- Migration, asylum & border control management
- Administration of justice & democratic processes, institutions & discourse

Criteria for risk assessment → **Examples of concrete high-risk use cases** → **Sensitive areas**

The compliance and enforcement system

Pre-market – conformity assessment

AI that is safety component of products (regulated by product legislation)

→ **conformity assessment** (already existing under the relevant sectoral legislation)

Other high-risk AI systems ("stand-alone")

→ **Ex ante conformity assessment through internal checks ***

→ **Registration** (EU database)

Post-market

- **Market surveillance** (authorities)
- **Post-market monitoring** (providers)
- **Reporting system** for serious incidents (providers and users)
- **Re-assessment** by the provider in case of substantial changes to AI systems
- **Human oversight and monitoring** (users)

* Exception remote biometric identification

European Commission