AI
ARTIFICIAL
INTELLIGENCE

EXCELLENCE
& TRUST

European Commission 2021 Artificial Intelligence Package

Dr. Tatjana Evas and
Dr. Gabriele Mazzini and Salvatore Scalzo
DG CNECT, European Commission

AI for Good Webinar
AI Policy, Standards and Metrics for Automated Driving Safety
2 June 2021

Agenda

1. Introduction: EU regulation on AI: milestones

2. 2021 European Commission AI Package

   2.1. Proposal for an Artificial Intelligence Act
   - Why a horizontal Regulation on AI?
   - Main concepts and objectives
   - A risk-based approach – main requirements
   - Conformity Assessment and Governance structure
   - Measures to support innovation

   2.2. Coordinated Plan on AI
   - Overview
   - Testing and Experimentation framework
   - Funding

3. Next steps

1. Introduction: EC regulation on AI milestones

Artificial Intelligence – soft regulation, hard regulation, or let it be? The question on EU policy agenda since 2015

A number of preparatory actions and wide discussion with broad spectrum of stakeholders (2017 – 2021) → guidelines + strategy, but no legislation specific on AI

2021 European Artificial Intelligence Package

2. 2021 EC Artificial Intelligence Package

EXCELLENCE AND TRUST

- **Communication:** "*Fostering a European approach to AI*"
- **Coordinated Plan** on AI 2021 review
- **Proposal for a legal framework on Artificial Intelligence**

2.1. Proposal for the Artificial Intelligence Act (1)

Why a horizontal EU regulation on AI?

Complexity — **Opacity**
Unpredictability —
Autonomy — **Data**

Solid framework of EU legislation already in place at EU and national level

HOWEVER

Certain **specific features of AI** can make application and enforcement of the existing rules more challenging and generate **risks to safety and fundamental rights**

A **tailored regulatory response** needed

The Commission's **proposal for a regulatory framework on AI**

2.1. Proposal for the Artificial Intelligence Act (2) Main elements

It is a horizontal act (!) applies to all AI systems that fall into the scope irrespective of the sector and follows new legislative framework (NLF) model

1. Defines what AI system is

2. Defines what AI use cases and under what conditions (different level of risks) can be put on the market or used in EU or banned from the EU

3. For High-risk AI systems
   - Sets 5 key requirements (+ special rules for remote biometric identification systems)
   - Spells out obligations for providers and users
   - Defines relevant bodies and applicable processes before the AI system can be put on the market (e.g. standards, notifying authority, notified body, conformity assessment, certificates and registration)
   - Defines supervision and market surveillance mechanisms after AI system is put on the market
   - Sets governance mechanism

2.1. Proposal for the Artificial Intelligence Act (3) Key principles and concepts

1. Regulatory continuity to support innovation and provide legal certainty

- Build on the EU existing legislation, procedures and governance structures (i.e. existing conformity assessment procedures; market surveillance Regulation)

2. Future-proof

- Definition of AI and 2-step classification of the high risk use cases
- 'New approach' legislative logic: Harmonization of legal requirements and Standardization

3. Risk-based

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

4. Level playing field for EU and non-EU players

- Independent of origin of producer or user

2.1. Proposal for the Artificial Intelligence Act (4) Key principles and concepts

5. 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 → i.e. **product** legislation logic
- Aligned to vast EU acquis on product safety which shall be jointly applied (e.g. AI embedded in products), however the legislative logic is different for 'new approach' and 'old approach' legislation

AI system = product →

- **designed by humans**
- **to perform assigned functions**
- **in line with expected capabilities**

2.1. Proposal for the Artificial Intelligence Act (5) The scope – what and who is covered?

Definition of Artificial Intelligence Article 3 point 1 + Annex I

"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)

2.1. Proposal for the Artificial Intelligence Act (6) The scope – what and who is covered?

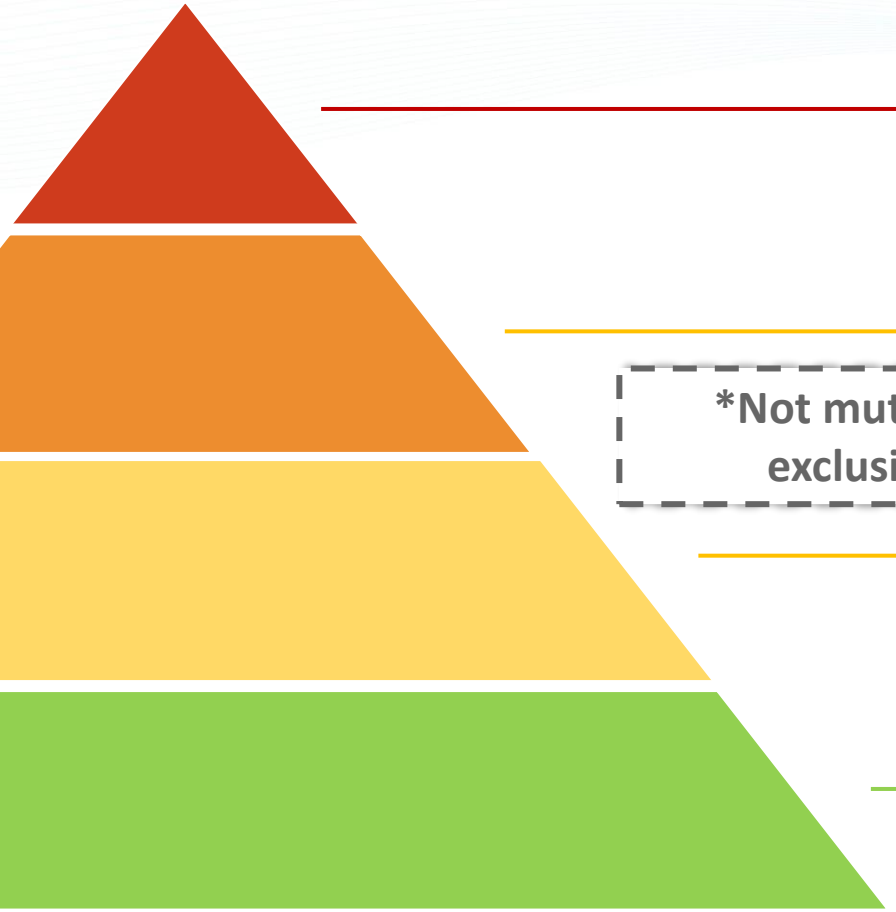
Regulation applicable to:

- **Providers (public or private)** placing on the market or putting into service AI systems in the Union independent from their origin
- **Users (public or private)** located within the Union
- **Providers and users** located in a third country, where the output produced by the system is used in the Union

Excluded from the scope:

- Public authorities in a third country or international organisations who use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States
- AI developed or used exclusively for military purposes

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



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

2.1. Proposal for the Artificial Intelligence Act (8)
Risk-based approach: minimal / no risk & 'transparency' risk

MINIMAL OR NO RISK

Transparency obligations for certain AI systems (Art. 52)

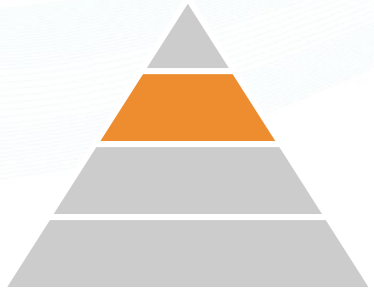
- **Notify humans** that they are **interacting with an AI system** unless this is evident
- **Notify humans** that they are **exposed to emotional recognition or biometric categorisation systems**
- Apply **label to deep fakes**

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)**

2.1. Proposal for the Artificial Intelligence Act (9) Risk-based approach: high risk AI systems

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



New Approach

Old Approach (automotive)

1 SAFETY COMPONENTS OF REGULATED PRODUCTS

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

2 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

Article 8 - Compliance with the requirements

1. High-risk AI systems shall comply with the requirements established in this Chapter.

2. The **intended purpose of the high-risk AI system** and the **risk management system** referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.

2.1. Proposal for the Artificial Intelligence Act (10) Requirements for high-risk AI systems

Establish and implement **risk management** processes

&

In light of the **intended purpose** of the AI system

Art. 10
Use high-quality **training, validation and testing data** (relevant, representative etc.)

Art. 11 + 12
Establish **documentation** and design logging features (traceability & auditability)

Art. 13
Ensure appropriate certain degree of **transparency** and provide users with **information** (on how to use the system)

Art 14
Ensure **human oversight** (measures built into the system and/or to be implemented by users)

Art. 15
Ensure **robustness**, **accuracy** and **cybersecurity**

Article 3(12) – intended purpose of AI system

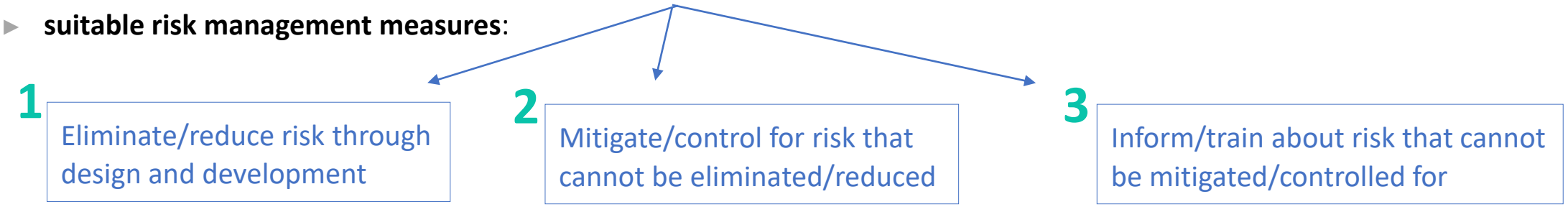
> ‘intended purpose’ means the **use for which an AI system is intended by the provider**, **including the specific context and conditions of use**, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

- **Key concept to AI Act proposal**
  - Common to EU product legislation → the product shall be safe and compliant when used in accordance with the product information
  - Relevant for classification as high-risk (Art. 6 and Annex III and amendment thereof)
  - Relevant for compliance with requirements (always taking into account intended purpose)
  - Relevant for risk management
  - Relevant for determination of ‘substantial modification’
  - Relevant for determination of ‘foreseeable misuse’
  - …

Article 9 - Risk management system

- **General principle widely used** in production and manufacturing processes and explicitly **foreseen in EU product legislation** (e.g. Annex I, point 1 Dir. 2006/42/EC (Machinery); Annex I, Ch. I Reg. 2017/745 (Medical Devices)
  - Basis for further standardisation already exists (e.g. ISO 31000, ISO/IEC/IEEE 16085:2021)

- Continuous iterative process throughout the entire lifecycle of AI system
  - **identification and evaluation** of known and foreseeable risks associated with AI system, including after placing on the market (through post-market monitoring)
  - **suitable risk management measures**:



"due consideration to the **effects and possible interactions resulting from the combined application of the requirements**" and taking "into account the **generally acknowledged state of the art**"

- **Obligation to test AI systems** for the purpose of identifying the most appropriate risk management measures

European Commission

2.1. Proposal for the Artificial Intelligence Act (11)

Integration of the requirements for the HR AI systems into the current legislation

NLF

The AI system will be high-risk if it is a safety component of a product or a device that is subject to a third party conformity assessment under the NLF legislation.

Requirements and obligations for high-risk AI systems set by the AI horizontal framework will become **directly applicable and will automatically complement the existing NLF legislation.**

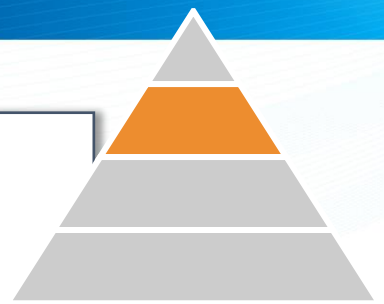
Old Approach

AI systems that are safety components of products under relevant old approach legislation will always be considered **high-risk.**

The new requirements for high-risk AI systems set by the AI horizontal framework **will have to be taken into account when adopting relevant implementing or delegated legislation under those acts**. (e.g. Art. 76 in relation to Reg. 167/2013)

2.1. Proposal for the Artificial Intelligence Act (12)

Overview: obligations of operators of HR systems (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

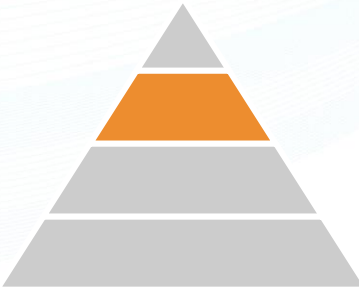
User obligations

- 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)

2.1. Proposal for the Artificial Intelligence Act (13) CE Marking of high-risk AI systems

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

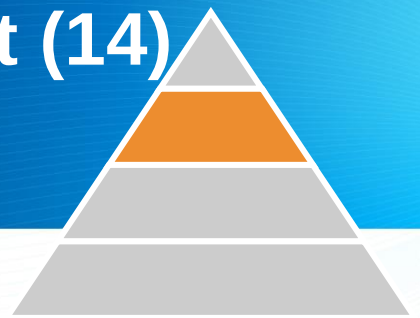
2 **Ensure** design and development and quality management system are **in compliance with the AI Regulation**

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**

2.1. Proposal for the Artificial Intelligence Act (14)
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

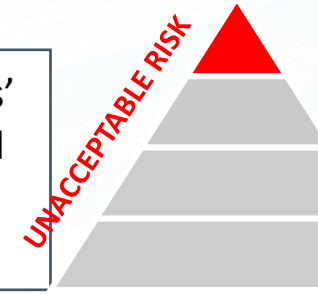
Human oversight and monitoring (users)

* Exception remote biometric identification

2.1. Proposal for the Artificial Intelligence Act (15)
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.**

2.1. Proposal for the Artificial Intelligence Act (16)
AI that contradicts EU values are prohibited



✗ **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.

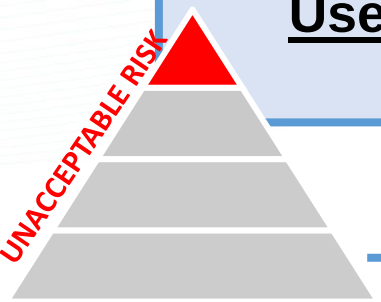
✗ **General purpose social scoring**

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.

2.1. Proposal for the Artificial Intelligence Act (17) Specific regulation on remote biometric identification



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

2.1. Proposal for the Artificial Intelligence Act (18) Measures to support innovation

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

2.1. Proposal for the Artificial Intelligence Act (19) The governance structure

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

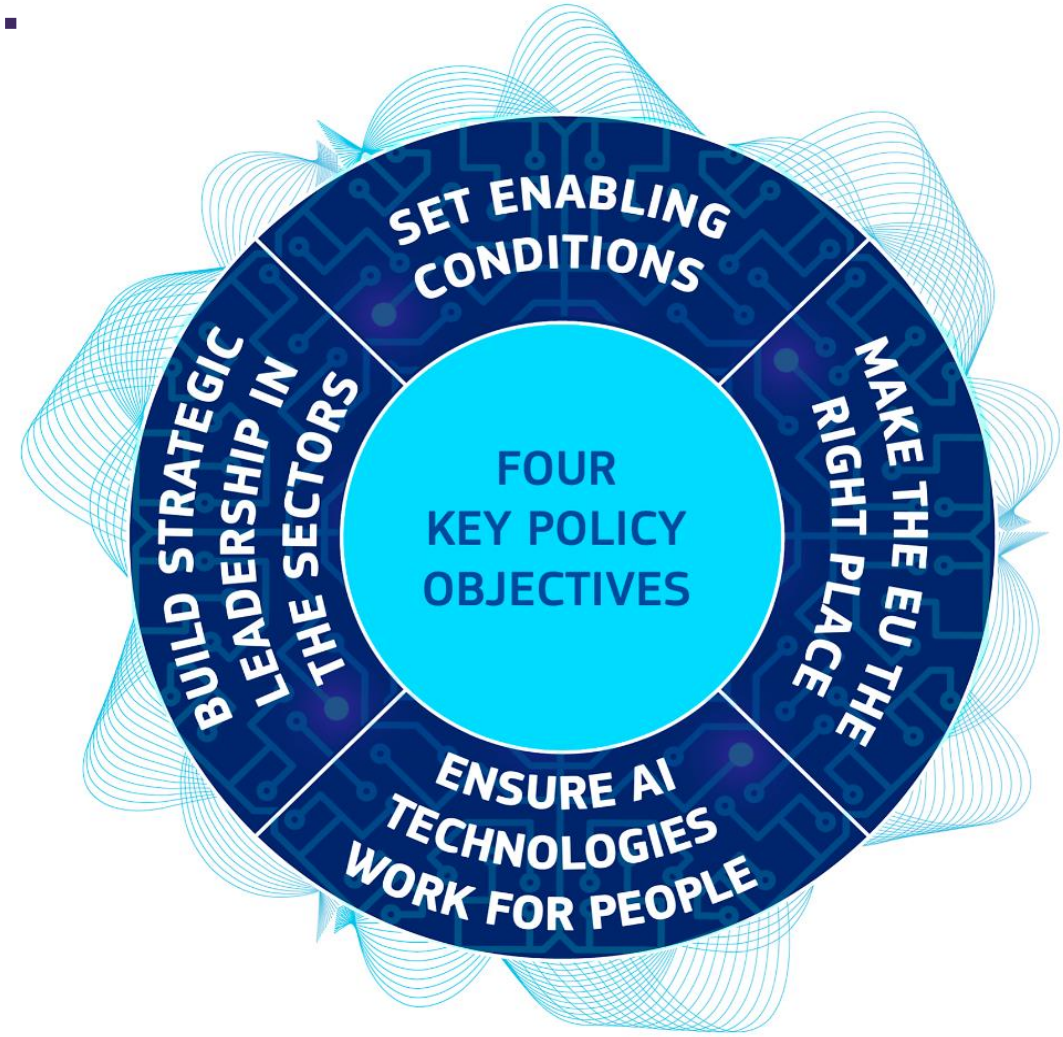
2.2. Coordinated Plan on AI – 2021 Review (1)
Boosting excellence in AI

The 2021 Coordinated Plan on AI:

- Operational **action plan to foster AI leadership in AI together with Member States**

- **Key messages:**

  - **Accelerate AI investments**
  - **Act on AI strategies**
  - **Align AI policies**



2.2. Coordinated Plan on AI – 2021 Review (2)

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

2.2. Coordinated Plan on AI – 2021 Review (3) Funding

- Target: € 20 billion per year public and private sector investment in AI
- Coordinated public efforts help leverage private investments

Digital Europe Programme	Build the strategic **digital capacities**, facilitate the wide **deployment of digital technologies**	**€ 2.1 billion for AI**	*2021 – 2027*
Horizon Europe Programme	Support **research and innovation** for new knowledge and innovative solutions	**€ 2.6 billion for AI** (estimated)	*2021 – 2027*
Recovery and Resilience Facility	Support Member States' **investments and reforms for recovery**	**20%** of the total **€ 670 billion** earmarked for digital, including AI	*2021 – 2026*

3. Next Steps

Artificial Intelligence Act

1

- The European Parliament and the Council as co-legislators will negotiate the proposal and agree on a compromise in the ordinary legislative procedure

2

- Once adopted, there will be 2 years of transitional period before the **Regulation becomes directly applicable** across the EU.

3

- In parallel, **harmonized standards of CEN/CENELEC** should be ready and support operators in the practical implementation of the new rules& conformity assessment procedures

Coordinated Plan on AI - Accelerate, Act and Align

AI
ARTIFICIAL
INTELLIGENCE

EXCELLENCE
& TRUST

Thank you!