Just in Time

European Commission

Regulation on Artificial Intelligence

Oct 2021

iason ESSENTIAL SERVICES FOR FINANCIAL INSTITUTIONS

Executive Summary

In April 2021, the **European Commission** published a **proposal for a Regulation on Artificial Intelligence (AI)** which introduces a **comprehensive, harmonized, regulatory framework for AI**.

The regulatory proposal aims to provide **AI developers, deployers and users** with clear requirements and obligations regarding specific uses of AI. At the same time, the proposal seeks to reduce administrative and financial burdens for business, in particular small and medium-sized enterprises (SMEs).

The proposed rules, based on a **future-proof approach**, will:

- Address risks specifically created by AI applications
- Propose a list of high-risk applications
- Set clear requirements for AI systems for high risk applications
- Define specific obligations for AI users and providers of high risk applications
- Propose a conformity assessment before the AI system is put into service or placed on the market
- Propose enforcement after such an AI system is placed in the market
- Propose a governance structure at european and national level

At a Glance

01	Introduction	4
02	Risk Based Approach	10
03	Measures in Support of Innovation	27
04	Governance and Innovation	30
05	Final Remarks	37
06	Annex	40

01

Introduction

AI: Benefits and Risks

Regulatory Framework: Balanced Approach

EC Proposal

EC Proposal: Risk-based and Future-proof Approach

Introduction 1/5

AI: Benefits and Risks

Artificial Intelligence (AI) is a **fast-evolving family of technologies** that can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities.

The use of artificial intelligence can support socially and environmentally beneficial outcomes and provide **key competitive advantages** to companies and the European economy.

However, the same elements and techniques that power the socio-economic benefits of AI can also bring about **new risks** or negative consequences for individuals or the society:

- Safety and security
- Fundamental rights
- Harder verifying compliance with the existing rules
- Legal uncertainty for companies
- Lack of trust by businesses and citizens
- Regulatory responses that fragment EU market

Introduction 2/5

Regulatory Framework: Balanced Approach

In light of the speed of technological change and possible challenges, the EU is committed to strive for a **balanced approach**:

"It is in the Union interest to preserve the EU's technological leadership and to ensure that Europeans can benefit from new technologies developed and functioning according to Union values, fundamental rights and principles".

This EC regulatory proposal:

1. Defines **common mandatory requirements** applicable to the design and development of certain AI systems **before they are placed on the market** that will be further operationalized through harmonized technical standards.

2. Addresses the situation **after AI systems have been placed on the market** by harmonizing the way in which **ex-post controls** are conducted.

Introduction 3/5

Regulatory framework: Objectives

The Commission puts forward the proposed regulatory framework on Artificial Intelligence with the following **specific objectives**:

Ensure that AI systems placed and used on the Union market are **safe and respect existing law** on fundamental rights and Union values

Ensure legal certainty to facilitate investments and innovation in AI

Enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems

Facilitate the **development of a single market for lawful, safe and trustworthy** AI applications and prevent market fragmentation

To achieve the objectives proposed, this proposal presents a **regulatory approach limited to the minimum necessary requirements** without:

- unduly **constraining and hindering technological development**
- disproportionately **increasing the cost of placing AI solutions** on the market.

Introduction 4/5

EC Proposal

The objectives of this **proposal can be better achieved at Union level**.

A solid European regulatory framework for trustworthy AI will also ensure a level playing field and protect all people, while strengthening Europe's competitiveness and industrial basis in AI.

The **European Parliament and the Member States** will need to **adopt the Commission's proposals** on a European approach for Artificial Intelligence and on Machinery Products in the ordinary legislative procedure and, even, **should be integrated into the existing obligations and procedures under Directive 2013/36/EU (CRD IV).**

Once adopted, the Regulations will be **directly applicable across the EU**.

In parallel, the Commission will continue to **collaborate with Member** States to implement the actions announced in the **Coordinated Plan**.

- Member States will have to **designate one or more national competent authorities (NCAs)** for the purpose of supervising the application and implementation of the regulation.
- The **European Artificial Intelligence Board** is a cooperation mechanism of governance, that will collect and share expertise and best practices among Member States, contribute to uniform administrative practices in the Member States, issue opinions or recommendations on this Regulation.
- The **European Data Protection Supervisor** will act as the competent authority for the supervision of the Union institutions, agencies and bodies.

Introduction 5/5

EC Proposal: Risk-based and Future-proof Approach

The proposal is based on a **risk-based and future-proof approach**:

- **Certain particularly harmful AI practices shall be prohibited** as contravening Union values
- **Predictable, proportionate and clear obligations** shall be also placed on providers and users of **high-risk systems**.

This proposal lays down obligation that will **apply to providers and users** of high-risk AI systems:

For **providers** who develop and place such systems on the Union market, it will create legal certainty and ensure that no obstacle to the cross-border provision of AI-related services and products emerge.

For **companies using AI**, it will promote trust among their customers.

For **national public administrations**, it will promote public trust in the use of AI and strengthen enforcement mechanisms.

Moreover, **the framework will envisage specific measures supporting innovation**.

02

Risk Based Approach

Risk Levels

Unacceptable Risk: Prohibited AI Practices

High-Risk: Classification

High-Risk: Requirements

High-Risk: Obligations of Providers

High-Risk: Conformity Assessment

High-Risk: Obligations of Stakeholders

High-Risk: Certificates, EU Declaration of Conformity and CE Marking of Conformity

High and Limited Risk: Transparency Obligations

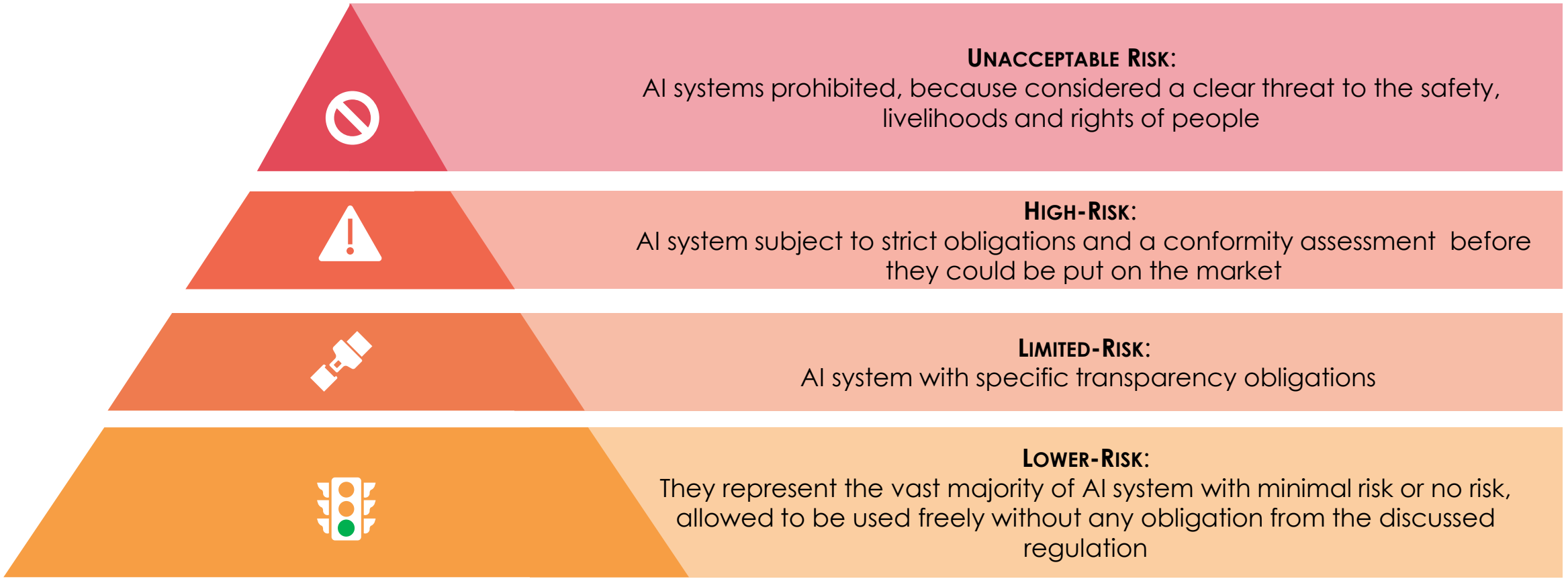
Limited and Lower Risk: Codes of Conduct

Notifying Authorities

Notifying Bodies

Risk Based Approach 1/16

Risk Levels

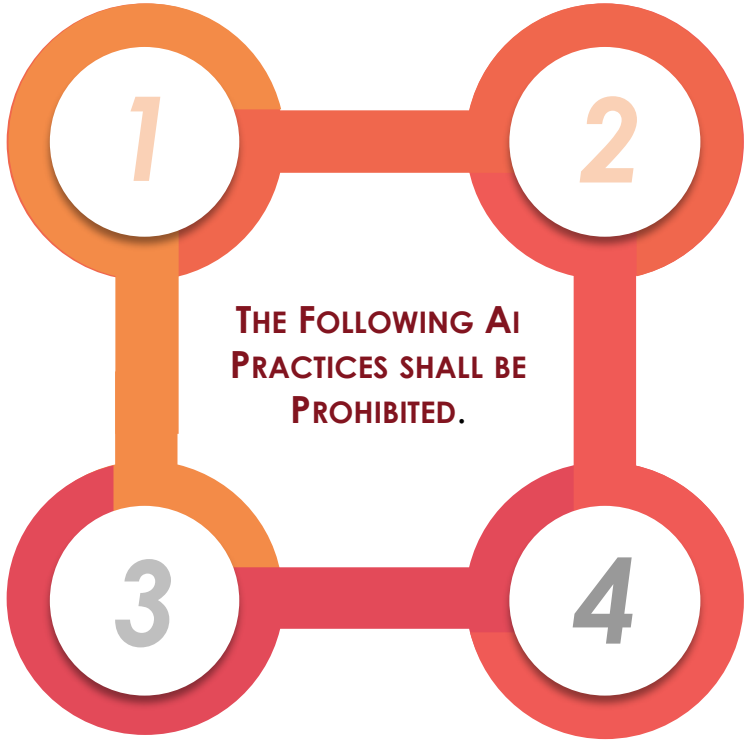


Risk Based Approach 2/16

Unacceptable Risk: Prohibited AI Practices

The placing on the market, putting into service or use of an AI system that **deploys subliminal techniques beyond a person's consciousness** in order to materially **distort a person's behavior.**

The placing on the market, putting into service or use of AI systems by public authorities or on their behalf for **the evaluation or classification of the trustworthiness of natural persons** with a consequent **social score leading to** detrimental or **unfavorable treatment** of certain natural persons or whole groups*.



The placing on the market, putting into service or use of an AI system that **exploits any of the vulnerabilities of a specific group of persons** in order to materially **distort the behavior of a person** pertaining to that group.

The use of **'real-time' remote biometric identification systems in publicly accessible spaces** for the purpose of law enforcement, unless and in as far as such use is strictly necessary.

*AI systems for the classification and evaluation of natural persons can be used (High Risk) when any prejudicial treatment, to which the natural person is subjected, is proportionate and / or justified with respect to his social behavior or its severity

Risk Based Approach 3/16

High-Risk: Classification

AI systems shall be considered high-risk where **both of the following conditions** are fulfilled:

- The **AI system** is intended to be **used as a safety component of a product, or is itself a product**, covered by the Union harmonization legislation;
- **The product is required to undergo a third-party conformity assessment** with a view to the placing on the market or putting into service of that product.

In addition to the previous, AI systems listed in any of the following areas shall also be considered high-risk*

- Biometric identification and categorization of natural persons (non-publicly accessible spaces)
- Management and operation of critical infrastructure
- Education and vocational training
- Employment, workers management and access to self-employment
- Access to and enjoyment of essential private services and public services and benefit
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes

* more details can be found in the annex of this document.

Risk Based Approach 4/16

High-Risk: Requirements 1/2

High-risk AI systems shall comply with certain requirements. The **risk management system** shall be considered when **ensuring compliance with those requirements.** The risk management system shall consist of a **continuous iterative process run throughout the entire lifecycle of a high-risk AI system** in order to **identify, analyze, estimate and evaluate risks related to high-risk AI systems.**

- ✓ Training, validation and testing data sets shall be subject to appropriate **data governance** and **management** practices.
- ✓ Training, validation and testing data sets shall be **relevant**, **representative**, **free of errors and complete**.
- ✓ Training, validation and testing data sets shall consider the **characteristics or elements that are particular to the specific geographical, behavioral or functional setting** within which the high-risk AI system is intended to be used.
- ✓ To the extent that it is strictly necessary for the purposes of ensuring bias monitoring of high-risk AI systems, the providers of such systems may **process special categories of personal data**

- ✓ The technical documentation of a high-risk AI system shall be drawn up **before that system is placed on the market** or put into service and shall be kept up-to date.

- ✓ The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system **complies with these requirements** and provide national competent authorities and notified bodies with **all the necessary information** to assess the compliance of the AI system with those requirements

Risk Based Approach 5/16

High-Risk: Requirements 2/2

Recording Keeping

- ✓ High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('**logs**') while the high-risk AI systems is operating. Furthermore, logging capabilities **ensure a level of traceability** of the AI system's functioning throughout its lifecycle.
- ✓ The logging capabilities shall provide:
  - Start **date** and end date of each use;
  - the reference **database**;
  - **Input data;**
  - The identification of the **natural persons** involved in the verification of the results.

Transparency & Oversight

- ✓ High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to **interpret the system's output** and use it appropriately. Furthermore, AI systems shall be accompanied by **instructions for use** accessible and comprehensible to users.
- ✓ High-risk AI systems shall be designed and developed in such a way that they can be effectively **overseen by natural persons** during the period in which the AI system is in use. Human oversight shall aim at preventing or **minimising the risks** to health, safety or fundamental rights that may emerge when a high-risk AI system is used.

Accuracy, Robustness and Cybersecurity

- ✓ High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness and cybersecurity. The **levels of accuracy** and the relevant accuracy metrics of high-risk AI systems shall be **declared in the accompanying instructions of use.**
- ✓ High-risk AI systems shall be **resilient as regards errors, faults or inconsistencies** that may occur within the system or the environment in which the system operates.
- ✓ High-risk AI systems shall be **resilient as regards attempts by unauthorized third parties** to alter their use or performance by exploiting the system vulnerabilities.

Risk Based Approach 6/16

High-Risk: Obligations of Providers 1/4

Before placing a high-risk AI system on the market, providers shall demonstrate the compliance of the system with the mandatory requirements. In order to place on the market or put into service a trustworthy AI system, are imposed other obligations for providers.

Risk Based Approach 7/16

High-Risk: Obligations of Providers 2/4

Compliance

- Providers shall ensure that their high-risk AI systems are compliant with the mandatory requirements.

Quality Management System (QMS)

- Providers shall put a quality management system to ensure compliance with the overall regulation;
- This QMS should be proportionate to the size of the provider's organization;
- For *credit institutions*, the obligation for a QMS shall be deemed to be fulfilled by complying with the rules on internal governance arrangements*.

Technical Documentation

- Providers shall draw up the technical documentation with detailed information of elements of AI system and process for its development;
- For credit institutions, they shall maintain the technical documentation as part of internal governance, arrangements and process*.

* Regulated by Directive (CRD IV) 2013/36 EU, Article 74

Risk Based Approach 8/16

High-Risk: Obligations of Providers 3/4

KEEP LOG AUTOMATICALLY GENERATED

- Providers shall keep the logs automatically generated (under their control, even with contractual arrangements) by them high-risk AI systems;
- The logs shall be kept for a period appropriate in the light of intended of high-risk AI system and applicable legal obligation (European or national);
- Credit institutions shall maintain the logs automatically generated as part of documentation of internal governance, arrangements and process*.

CONFORMITY ASSESSMENT

- AI systems shall undergo a conformity assessment (see in following slides) prior of them placement on the market;
- For AI system intended to be used for creditworthiness assessment of natural person by credit institutions, the assessment should be carried out as part of the SREP**.

REGISTRATION

- Before placing on the market or putting into service a high-risk AI system, providers shall register it in the EU database.

* Regulated by Directive (CRD IV) 2013/36 EU, Article 74
** Regulated by Directive (CRD IV) 2013/36 EU, from Article 97 to 101

Risk Based Approach 9/16

High-Risk: Obligations of Providers 4/4

Corrective Actions

- Providers, which consider that one of them AI system placed on the market is not compliant with the overall regulation, shall immediately take the necessary corrective action, to withdraw it or to recall it, as appropriate;
- They shall inform the distributors of the high-risk AI system and the authorized representative and importers.

CE Marking of Conformity

- The CE marking of conformity shall be affixed visibly, legibly and indelibly or affixed on the high-risk AI system (further details in the following slides).

Duty of Information

- When the AI high-risk system presents a risk at a national level and the provider shall immediately inform the NCAs and, where applicable, the notified body that issued a certificate for that system.

Cooperation with NCA

- Upon a reasoned request by a NCA, providers shall deliver to it all information and documentation necessary to demonstrate the AI system conformity;
- If reasonably requested, providers shall give the access to the logs automatically generated by the AI system to the extent of log under them control.

Risk Based Approach 10/16

High-Risk: Conformity Assessment

Type of High-risk AI System	Conformity Assessment
▪ Biometric identification and categorization of natural person	Two different type of conformity assessment: ▪ Conformity assessment based on **internal control** (only for those providers that have applied harmonized standards or common specifications of the European Commission); ▪ Assessment of the QMS and the technical documentation **with the involvement of a notified body.**
▪ Management and operation of critical infrastructure ▪ Education and vocational training ▪ Employment, workers and access to self-employment ▪ Access to and enjoyment of essential private and public services and benefits ▪ Law enforcement ▪ Migration, asylum and border control management ▪ Administration of justice and democratic processes	Providers shall follow the conformity assessment procedure based on **internal control**, which does not provide the involvement of a notified body. For high-risk Ai systems intended to be used to evaluate the **creditworthiness of natural persons** or establish their credit score placed on the market or put into service by credit institutions, the conformity assessment shall be carried out as part of the procedure of part of the SREP.
▪ High-risk AI system, to which legal acts lies on the EU harmonization legislation	The provider shall follow the relevant conformity assessment **as required under those legal acts** (and are applied also the high-risk AI system requirements).

Risk Based Approach 11/16

High-Risk: Obligations of Stakeholders

Importers

Before placing on the market an AI system, they shall:

- ensure that provider carried out **the appropriate conformity assessment**;
- **not place on the market** if they consider that the AI system does not comply with the regulation;
- **inform the provider** and the market surveillance authorities if the AI system present a risk at national level;
- **cooperate** with NCAs.

Distributors

They shall:

- **verify** that the AI system bears **the CE conformity marking**, is accompanied by the **required documentation** and **instructions of use**;
- **not place on the market** an AI system, if they consider that it isn't compliant with the regulation;
- **take the corrective action**, **withdraw** or **recall** the AI system, **ensure that the provider/importer take the corrective actions** if they consider that an AI system made available on the market is not compliant with the regulation;
- **cooperate** with NCAs.

Authorized Representatives

If an importer cannot be identified, the provider appoint an authorized representative (AR) **established in the Union**. The AR shall perform the tasks specified in the mandate, in particular:

- **Keep a copy of declaration of conformity and the technical documentation** at the disposal of NCAs;
- Upon a reasoned request, **provide all the information for demonstrate conformity** to NCAs
- cooperate with NCAs;

Users

They shall:

- use the AI system **in accordance with the instructions of use** and **monitor** the operations of the AI system;
- **inform** the provider/distributor and **interrupt** the use of the AI system, if they identify **incidents or malfunctioning**;
- **Inform** the provider/distributor and **suspend** the use of the AI system, If they consider that the use present a **risk at a national level**;
- **Keep the logs automatically generated** by the AI system;

Risk Based Approach 12/16

High-Risk: Certificates, EU Declaration of Conformity and CE Marking of Conformity

Certificates

Certificates are issued by notified bodies after the assessment of conformity with the mandatory Requirements;

—

They shall be valid for the period they indicate, which shall not exceed five years;

—

Where notified bodies finds that an AI system no longer comply with the requirements, they shall suspend, withdraw or impose restrictions on the certificate issued.

EU Declaration of Conformity

Providers shall draw a written EU declaration of conformity for each AI system and keep it at the disposal of NCAs;

—

The EU declaration of conformity shall state that the high-risk AI system in question is compliant with its requirements;

—

With the EU declaration of conformity, providers shall assume responsibility for compliance with the high-risk AI systems requirements..

CE Marking of Conformity (CE)

The CE marking of conformity shall be affixed visibly, legibly and indelibly or affixed on the high-risk AI system;

—

Where it is not possible, the CE marking of conformity shall be affixed to the packaging or to the accompanying documentation;

—

The CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment.

Risk Based Approach 13/16

High and Limited Risk: Transparency Obligations

For limited-risk AI system (and high-risk AI system) are set some obligations for providers, in order to ensure transparency and the awareness of natural persons that interact with those systems

1. Providers shall ensure that AI system intended to interact with natural persons are designed and developed in such a way **that natural persons are informed that they are interacting with an AI system**.

2. Users of an emotion recognition system or a biometric categorization system **shall inform of the operation of the system the natural persons exposed thereto.**

3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful, **shall disclose that the content has been artificially generated or manipulated**

Risk Based Approach 14/16

Limited and Lower Risk: Codes of Conduct

The development of AI systems, other than high-risk AI systems, in accordance with the requirements of this Regulation may lead to a larger uptake of trustworthy artificial intelligence in the Union:

Providers of **non-high-risk AI systems** should be encouraged to **create codes of conduct** intended to foster the application of the mandatory requirements applicable to high-risk AI systems

Providers should also be encouraged to apply on a **voluntary basis additional requirements** (for example related environment, social and governance factors)

It is important that AI systems related to products that are not high-risk are nevertheless safe when placed on the market or put into service.

IMPACT ASSESMENT

Businesses or public authorities that develop or use any AI applications **not classified as high risk would not have to incur any costs, if not those related to voluntary codes of conduct.**
In these cases, costs could be as high as for high-risk applications at most, but most probably lower.

Risk Based Approach 15/16

Notifying Authorities

Definition

«**Notifying authority**» means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and **notification of conformity assessment bodies** and for their monitoring:

- **Each Member State** shall designate or establish a notifying authority (they may designate a national accreditation body);
- Notifying authorities shall be established, organized and operated in such a way that **no conflict of interest** arises with conformity assessment bodies.

Notification

Conformity assessment bodies shall apply for **notification to the notifying authority** of the Member State in which they are established. The application for notification shall be accompanied by:

- A **description** of the conformity assessment **activities**, the conformity assessment **modules** and the **AI technologies** for which the conformity assessment body claims to be competent;
- an **accreditation certificate**, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements for notified bodies;
- Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with the **documentary evidence** necessary for the verification, recognition and regular monitoring of its compliance with the requirements for notified bodies.

Notification Procedure

Notifying authorities may **notify** only conformity assessment bodies which have satisfied the requirements for notified bodies:

- Notifying authorities shall notify the Commission and the other Member States **using the electronic notification tool** developed and managed by the Commission;
- The notification shall include full **details** of the conformity assessment **activities**, the conformity assessment **modules** and the **AI technologies** concerned;
- Notifying authorities shall **notify the Commission** and the other Member States of any subsequent relevant **changes to the notification**.

Risk Based Approach 16/16

Notified Bodies

Definition	Requirements	Challenge to Competence of Notified Bodies
«**Notified body**» means a conformity assessment body to **verify the conformity of high-risk AI system**. It designated in accordance with this Regulation and other relevant Union harmonization legislation.	▪ The Commission make available **the list of the notified bodies**, including the identification numbers and the activities for which they have been notified; ▪ Notified bodies shall **satisfy** the organizational, quality management, resources and process **requirements** that are **necessary to fulfil their tasks;** ▪ The organizational structure, allocation of responsibilities, reporting lines and operation of notified bodies shall ensure that there is **confidence in the performance and in the results of the conformity assessment activities** conducted by the notified bodies; ▪ Notified bodies shall operate so as to safeguard the **independence, objectivity and impartiality** of their activities; ▪ Notified bodies shall have documented procedures in place ensuring the **confidentiality of the information** in their possession; ▪ Notified bodies shall make available and **submit** upon request all **relevant documentation** to the notifying authority.	▪ Where a **notifying authority** has **suspicions** or has been informed that a **notified body no longer meets the requirement**s, or that it is failing to fulfil its obligations, that authority shall **without delay investigate** the matter with the utmost diligence; ▪ Where the Commission **ascertains** that a **notified body** does not meet or **no longer meets the requirements**, it shall adopt a reasoned decision requesting the notifying Member State to **take the necessary corrective measures**, including withdrawal of notification if necessary.

03

Measures in Support of Innovation

AI Sandboxes: Definition & Functioning

Measures for Small-scale Providers and Users

Measures in Support of Innovation 1/2

AI Sandboxes: Definition & Functioning

Just in Time

DEFINITION

Sandboxes are **environments** monitored and controlled by authorities for the **development and testing** of innovative AI systems under strict regulatory oversight, before these systems are placed on the market or otherwise put into service.

1. The AI regulatory sandboxes shall not affect the **supervisory and corrective** powers of the competent authorities.
2. Participants in the AI regulatory sandbox (big providers and SMEs) shall remain liable under applicable Union and Member States liability legislation for any **harm inflicted** on third parties as a result from the **experimentation** taking place in the sandbox.
3. Member States' competent authorities that have established AI regulatory sandboxes shall **coordinate their activities and cooperate** within the framework of the **European Artificial Intelligence Board.**
4. The modalities and the conditions of the operation of the AI regulatory sandboxes, and the rights and obligations of the participants shall be set out in **implementing acts.**

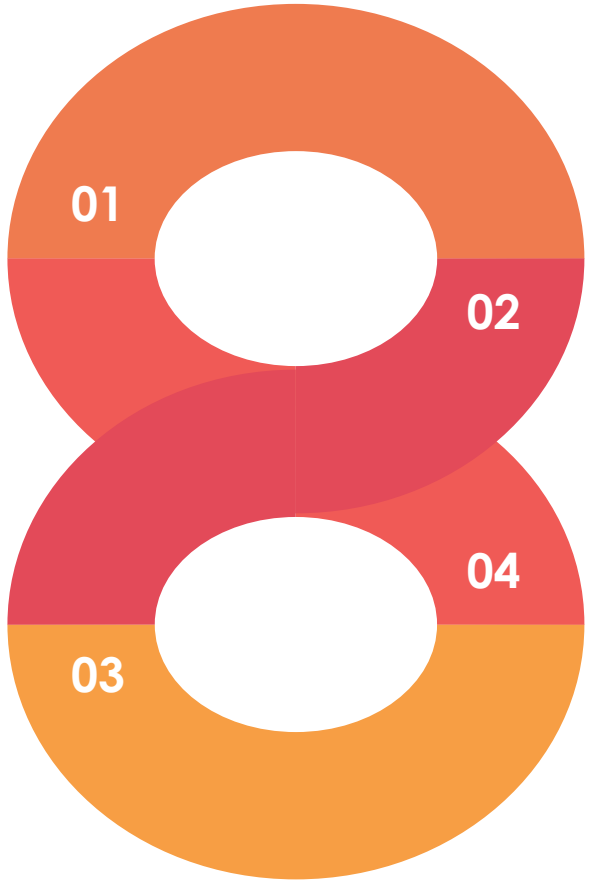
Measures in Support of Innovation 2/2

Measures for Small-scale Providers and Users

In order to promote and protect innovation, it is important that the interests of **small-scale providers and users** of AI systems are considered. To this objective, Member States should develop initiatives that would help these actors in the following ways:

01. Access to AI Sandboxes

Provide small-scale providers and start-ups with **priority access** to the AI regulatory sandboxes to the extent that they fulfil the **eligibility conditions.**



02. Awareness Activity

Organize specific **awareness raising activities** about the application of this Regulation tailored to the needs of the small-scale providers and users

03. Channel for communication

Where appropriate, establish a **dedicated channel for communication** with small-scale providers and user and other innovators to provide guidance and respond to queries about the **implementation** of this Regulation.

04. Assessment fees

The specific interests and needs of the small-scale providers shall be considered when setting **the fees for conformity assessment** under Article 43, reducing those fees proportionately to their size and market size.

04

Governance and Innovation

European Artificial Intelligence Board

National Competent Authorities

EU Database for Stand-alone High-risk AI Systems

Post Market Monitoring and Sharing of Information

Enforcement

Governance and Innovation 1/6

European Artificial Intelligence Board 1/2

The proposed rules will be **enforced** through a governance system at Member States level, building on already existing structures, and a cooperation mechanism at Union level with the establishment of a **European Artificial Intelligence Board.** The Board will have the following tasks:

1. It will be responsible for a number of **advisory tasks**, including issuing opinions, recommendations, advice or guidance on matters related to the implementation of this Regulation, including **on technical specifications** or existing standards regarding the requirements established in this Regulation
2. **Collect and share expertise and best practices** among Member States in order to create a uniform way of acting across the Member States.
3. **Contribute to uniform administrative practices** in the Member States making easy to do comparison between Member States and adjust those states not in line with the administrative practices.

Governance and Innovation 2/6

European Artificial Intelligence Board 2/2

The **European Artificial Intelligence Board** is created with the following **objectives** and **structure**:

Objectives

Contribute to the effective **cooperation** of the national supervisory authorities and the Commission with regard to matters covered by this Regulation.

Coordinate and **contribute** to **guidance** and **analysis** by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market.

Assist the **national supervisory authorities** and the Commission in ensuring the consistent application of this Regulation.

Structure

The Board shall be composed of the **national supervisory authorities**, who shall be represented by the head or equivalent high-level official of that authority, and the European Data Protection Supervisor.

The Board shall be chaired by the **Commission**, who shall convene the meetings and prepare the agenda.

The Board may invite **external experts** and **observers** to attend its meetings and may hold exchanges with interested third parties to inform its activities to an appropriate extent.

Governance and innovation 3/6

National Competent Authorities

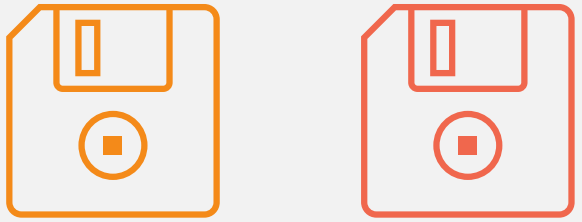
The EC proposal covers the **duties** and the **goals** of the national competent authorities. National competent authorities shall be **established** or **designated** by each Member State for the purpose of ensuring the application and implementation of this Regulation. Member States shall perform the following **tasks**:

- **Organize** national competent authorities as to **safeguard** the objectivity and impartiality of their activities and tasks.
- **Designate** a national **supervisory authority** among the national competent authorities.
- **Inform** the Commission of their **designation** or designations and, where applicable, the reasons for designating more than one authority.
- **Ensure** that national competent authorities are provided with adequate **financial and human resources** to fulfil their tasks under this Regulation.
- **Report** to the Commission on an annual basis on **the status** of the **financial and human resources** of the national competent authorities with an assessment of their adequacy.
- **Instruct** national competent authorities to provide **guidance and advice** on the implementation of this Regulation, including to small-scale providers.

Governance and innovation 4/6

EU Database for Stand-alone High-risk AI Systems

The Commission shall, in collaboration with the Member States, **set up and maintain an EU database** containing information on high-risk AI systems.



1 Information contained in the EU database shall be **accessible to the public.**

2 The EU database shall contain **personal data** only insofar as necessary for **collecting and processing information** in accordance with this Regulation

3 The Commission shall be the **controller** of the EU database. It shall also ensure to **providers adequate technical and administrative support.**

Governance and Innovation 5/6

Post Market Monitoring and Sharing of Information

The EC propose the **monitoring** and **reporting obligations** for providers of AI systems regarding post-market monitoring and reporting and investigating on AI-related incidents and malfunctioning:

Post-market Monitoring Establishment

Providers shall **establish** and **document** a post-market **monitoring system** in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.

Data Analysis

The post-market monitoring system shall actively and systematically **collect, document and analyze relevant data** provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime

Post/Market Monitoring

The post-market monitoring system shall be based on a **post-market monitoring plan**. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.

Incidents Reporting

Providers of high-risk AI systems placed on the Union market shall report any **serious incident or any malfunctioning** of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred. Such notification shall be made **immediately** after the provider has established a **causal link** between the AI system and

Governance and innovation 6/6

Enforcement

The national supervisory authority shall report to the Commission on a regular basis the outcomes of relevant **market surveillance** activities. Where the market surveillance authority of a Member State has sufficient reasons to consider that an AI system presents a **risk**, they shall carry out an **evaluation** of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation according to the following path:

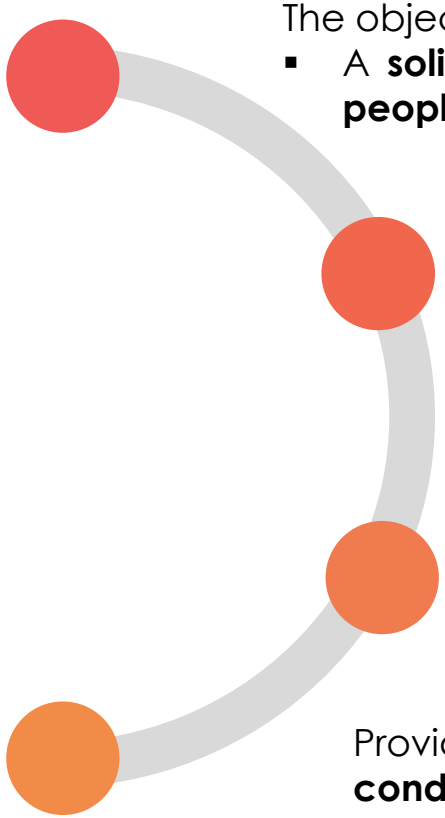
1. Where, during the evaluation, the market surveillance authority finds that the AI system does not **comply** with the **requirements** and obligations laid down in this Regulation, it shall without delay require the relevant operator to take all **appropriate corrective actions** to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a reasonable period.
2. Where the market surveillance authority considers that non-compliance is not restricted to its **national territory**, it shall inform the Commission and the **other Member States** of the results of the evaluation and of the actions which it has required the operator to take.
3. The **operator** shall ensure that all appropriate **corrective action** is taken in respect of all the AI systems concerned that it has made available on the market throughout the Union. .
4. Where the operator of an AI system does not take **adequate corrective action** within the period indicated, the market surveillance authority shall take all **appropriate provisional measures** to prohibit or restrict the AI system's being made available on its national market, to withdraw the product from that market or to recall it

05

Final Remarks

Final Remarks 1/2

Artificial Intelligence (AI) is a fast-evolving family of technologies that can bring a wide array of **economic and societal benefits** across the entire spectrum of industries and social activities but can also bring about **new risks or negative consequences** for individuals or the society.



The objectives of the EC proposal can be better achieved at Union level.

- A **solid European regulatory framework for trustworthy AI** will ensure a **level playing field** and **protect all people**, while strengthening **Europe's competitiveness and industrial basis in AI**.

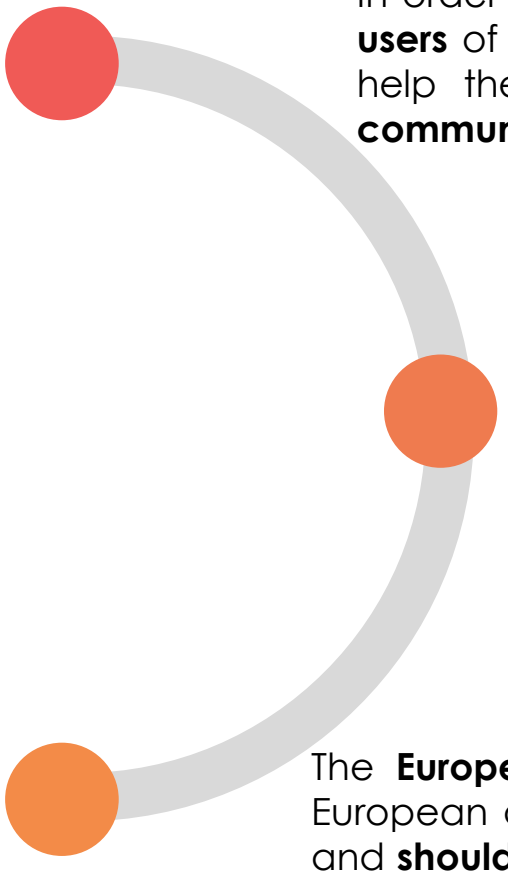
To be classified as **high-risk AI systems**:

- must be used as a safety component of a product and this product **is required to undergo a third-party conformity assessment**
- shall **comply with certain requirements** (Data, Documentation, Record – Keeping, Transparency, Oversight, Accuracy Robustness And Cybersecurity)

Some obligations are also provided for **limited-risk AI system**: they concerns about **users' awareness** of dealing with AI system

Providers of **non-high-risk AI systems** (Limited and Lower Risk) should be encouraged to create **codes of conduct** and **voluntary basis additional requirements**

Final Remarks 2/2



In order to promote and protect innovation, it is important that the interests of **small-scale providers and users** of AI systems are considered. To this objective, Member States should develop initiatives that would help these actors to get access to **AI sandboxes** together with big providers, enter **channel for communication**, **get aware of the AI activity**.

A **European Artificial Intelligence Board is set up**. The Board **collects and shares expertise and best practices** among Member States, **contributes to uniform administrative practices** in the Member States**, issues opinions or recommendations** on this Regulation.

The **European Parliament and the Member States** will need to **adopt the Commission's proposals** on a European approach for Artificial Intelligence and on Machinery Products in the ordinary legislative procedure and **should be integrated even into the existing obligations and procedures under Directive 2013/36/EU (CRD IV)**

06

Annex

High-Risk AI Systems Referred to in Article 6(2)

Annex 1/3

High-Risk AI Systems Referred to in Article 6(2) 1/3

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometric identification and categorization of natural persons:
    a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;

2. Management and operation of critical infrastructure:
    a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.

3. Education and vocational training:
    a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
    b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.

4. Employment, workers management and access to self-employment:
    a) 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;
    b) 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.

5. Access to and enjoyment of essential private services and public services and benefits:
    a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
    b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;
    c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

Annex 2/3

High-Risk AI Systems Referred to in Article 6(2) 2/3

6. Law enforcement:
    a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
    b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
    c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);
    d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence during investigation or prosecution of criminal offences;
    e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behavior of natural persons or groups;
    f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;
    g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

Annex 3/3

High-Risk AI Systems Referred to in Article 6(2) 3/3

7. Migration, asylum and border control management:
    a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
    b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;
    c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;
    d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. Administration of justice and democratic processes:
    a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

Company Profile

Iason is an international firm that consults Financial Institutions on Risk Management. Iason integrates deep industry knowledge with specialised expertise in Market, Liquidity, Funding, Credit and Counterparty Risk, in Organisational Set-Up and in Strategic Planning.

Alberto Bove Natellis

Matteo Cecchin

Ulisse Filipponi

This document was prepared in collaboration with Riccardo Chinello, who at the time was working for Iason Consulting.

www.iasonltd.com