Proposal for a Regulation laying down harmonised rules on Artificial Intelligence

European Commission

List of abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
CA	Competent Authorities
EC	European Commission
EP	European Parliament
EU	European Union
NCAs	National Competent Authorities

The Proposal for a Regulation on AI tabled by the EC on 21 April 2021 set harmonised rules for the development, placement on the market and use of AI systems in the EU following a proportionate risk-based approach

- On 19 February 2020 the EC published the White Paper on AI - **A European approach to excellence and trust**. The White Paper set out policy options on how to achieve the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of such technology.
- The EP and the EC have repeatedly expressed calls for legislative action to ensure a **well-functioning internal market** for AI systems where both **benefits and risks of AI are adequately addressed** at EU level.
- In October 2020, the EP **adopted a number of resolutions related to AI**, including on ethics, liability and copyright. In 2021, those were followed by resolutions on AI in criminal matters and in education, culture and the audio-visual sector.

In this context, the EC puts forward the **Proposal for a Regulation on AI,** in conjunction with a coordinated plan and a communication on fostering a European approach. The proposal has the following specific objectives:

- Ensure that AI systems placed on the EU market and used are safe and **respect existing law** on **fundamental rights** and **EU values**.
- Ensure **legal certainty** to facilitate investment 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 those objectives, this proposal presents a balanced and proportionate horizontal regulatory approach to AI.

Milestones in the regulation of AI

2020	2021	¿?
(Feb.) The Commission published the White Paper on AI (Oct.) EP adopted resolutions related to AI, including on ethics, liability and copyright	(Apr.) EC tabled its Proposal for a Regulation on AI[1]	(¿?) This Regulation must be adopted by the EP and the Council and It shall enter into force on the twentieth day following that of its publication in the Official Journal of the EU.

1 Proposal for a regulation laying down harmonised rules on AI, scope of this technical note .

2 Prohibited Artificial Intelligence practices

Main aspects

Prohibited AI practices are mainly focused on subliminal techniques, exploiting vulnerabilities, misuse by public authorities and some biometric identification systems uses in public

Prohibited practices

The placing on the market, putting into service or use of AI …

- … that deploys **subliminal techniques** beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm.
- … that exploits any of the **vulnerabilities of a specific group** of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm.
- … by public authorities or on their behalf for the evaluation or **classification of the trustworthiness of natural persons** over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading detrimental or unfavourable treatment of certain natural persons or whole groups thereof:
  - in social contexts which are unrelated to the contexts in which the data was originally generated or collected, or;
  - that is unjustified or disproportionate to their social behaviour or its gravity.

Remote biometric identification systems

- The use of "real-time" **remote biometric identification systems in public spaces** for the purpose of law enforcement shall be prohibited, unless they are necessary with one of the following objectives:
  - The targeted search for specific potential victims of crime.
  - Prevention specific, substantial and inminent threat to the life or physical safety of natural persons or of a terrorist attack.
  - Detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence and punishable in a Member State.
- The use of 'real-time' **remote biometric identification systems in publicly accessible spaces** for the purpose of law enforcement for any of the objectives referred to **shall take into account**:
  - The nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system.
  - The consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

3 High-Risk AI Systems
Classification

The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation. The classification as high-risk does not only depend on the function performed by the system, but also on the purpose and modalities for which that system is used

- There are specific rules for AI systems that create a high risk to the health and safety or fundamental rights of natural persons. In line with a risk-based approach, those **high-risk AI systems are permitted** on the European market subject to **compliance with certain mandatory requirements** and an ex-ante conformity assessment.

Classification of AI systems as high risks

- An AI system shall be considered **high-risk** where all 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 EU harmonisation legislation**.
  - The **product whose safety component is the AI system**, or the AI system itself as a 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 pursuant to the EU harmonisation legislation.
  - In addition to the previous high-risk AI systems, the regulation provides a list AI systems, with mainly **fundamental rights implications**, that shall be considered high risk (e.g. AI systems intended to be used for i) the remote biometric identification of persons in publicly accessible spaces; ii) as safety components in the management and operation of essential public infrastructure networks, such as roads or the supply of water, gas and electricity).

3 High-Risk AI Systems

Legal requirements and obligations

The intended purpose of the high-risk AI system and the risk management system shall be taken into account when ensuring compliance with those requirements. The providers of high-risk AI systems shall fulfill the obligations required

Legal requirements for high-risk AI systems

- The proposed **minimum requirements are largely consistent with other international recommendations and principles**, which ensures that the proposed AI framework is compatible with those adopted by the EU's international trade partners.
- A risk management system **shall be established, implemented, documented and maintained in relation to high-risk AI systems**.
- The risk management system shall consist of a **continuous iterative process run throughout the entire lifecycle** of a high-risk AI system. It shall comprise the following steps:

1. Identification and analysis of the known and foreseeable risks associated with each high-risk AI system.
2. Estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose.
3. Evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system.
4. Adoption of suitable risk management measures.

Obligations of providers of high-risk AI systems

- Providers of high-risk AI systems shall:
  - **Ensure that their high-risk AI systems are compliant with the legal requirements.**
  - Have a **quality management** system in place.
  - Draw-up the **technical documentation** of the high-risk AI system.
  - When under their control, keep the logs **automatically generated** by their high-risk AI systems.
  - Ensure that the high-risk AI system undergoes the **relevant conformity assessment procedure** prior to its placing on the market or putting into service.
  - Comply with the **registration obligations**.
  - Take the **necessary corrective actions**, if the high-risk AI system is not in conformity with the legal requirements.
  - Inform the NCAs of the Member States in which they made the AI system available of the non-compliance and of any **corrective actions taken**.

3 High-Risk AI Systems

Notifying authorities and notified bodies

A framework is needed for the notified bodies to be involved as independent third parties in conformity assessment procedures

- The framework for notification authorities, procedures an bodies is divided in the following sections:

Notifying authorities

- Each Member State shall designate or establish a **notifying 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.
- Notifying authorities **shall be established, organised and operated** in such a way that no conflict of interest arises with conformity assessment bodies and the objectivity and impartiality of their activities are safeguarded.
- Notifying authorities shall **not offer or provide any activities that conformity assessment bodies perform or any consultancy services** on a commercial or competitive basis.

Notification procedure

- Notifying authorities shall notify the EC and the other Member States using the **electronic notification** tool developed and managed by the EC.
- The notification shall include **full details of the conformity assessment activities**, the conformity assessment module or modules and the AI technologies concerned.

Notified bodies

- Notified bodies shall perform the conformity assessment of the high risk AI systems and **satisfy the organisational, quality management, resources and process requirements** that are necessary to fulfil their tasks.
- Notified bodies shall be **independent of the provider** of a high-risk AI system in relation to which it performs conformity assessment activities.

3 High-Risk AI Systems

Conformity assessment procedure

There is a conformity assessment procedure for each type of high-risk AI system. The procedure has the following key elements: harmonized standards, conformity assessments, certificates and registration

Key elements

- The conformity assessment approach aims to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time

1 Harmonised standards

- They aim to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time.
- **High-risk AI systems** which are in **conformity with harmonised standards** or parts thereof shall be presumed to be **in conformity with the legal requirements** for high-risk AI systems.

2 Conformity assessment

- They aim to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time.
- **High-risk AI systems** which are in **conformity with harmonised standards** or parts thereof shall be presumed to be **in conformity with the legal requirements** for high-risk AI systems.

3 Certificates

- They aim to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time.
- **High-risk AI systems** which are in **conformity with harmonised standards** or parts thereof shall be presumed to be **in conformity with the legal requirements** for high-risk AI systems.

4 Registration

- They aim to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time.
- **High-risk AI systems** which are in **conformity with harmonised standards** or parts thereof shall be presumed to be **in conformity with the legal requirements** for high-risk AI systems.

4 Transparency Obligations for certain AI systems

Main aspects

Certain AI systems require transparency obligations so that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use

Transparency obligations will apply for systems that:

- Interact with humans. Providers shall **ensure that AI systems are designed and developed in such a way that persons are informed that they are interacting with an AI system**.

- Are used to detect emotions or determine association with (social) categories based on biometric data. Users of an **emotion recognition system or a biometric categorisation** system shall inform of the operation of the system the natural persons exposed thereto.

- Generate or manipulate content (‘deep fakes’). 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.

- However, the **transparency obligations** in relation with the systems that interact with **humans shall not apply** where the use is authorised by law to detect, prevent, investigate and prosecute **criminal offences**.

5 Measures in Support of Innovation

AI regulatory sandboxes

To keep a legal framework that is sustainable over time and is innovation-friendly, the EC encourages to set up regulatory sandboxes and sets a basic framework in terms of governance, supervision and liability

AI **regulatory sandboxes** established by one or more Member States CAs or the European Data Protection Supervisor are expected to provide a **controlled environment that facilitates the development, testing and validation** of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan.

This is expected to take place under the direct **supervision and guidance** by the **CAs** with a view to ensuring **compliance with the requirements of this Regulation** and, where relevant, other Union and Member States legislation supervised within the sandbox.

All the **authorities competent in the protection of data** used in the innovative AI systems must be **included** in the operation of the **AI regulatory sandbox** of the same, which will be supervised by the member states.

Any significant risks to health and safety and fundamental rights **identified during the development and testing** of such systems shall result in immediate **mitigation and, failing that, in the suspension** of the process until such mitigation takes place, with participants in the AI regulatory sandbox being liable, where appropriate, for any harm inflicted on third parties.

Any **member state** establishing AI regulatory sandboxes is expected to **cooperate under the framework of the European Artificial Intelligence Board** through **annual reports** including experience obtained in all areas.

Member States are expected to undertake measures to **reduce the regulatory burden on small and medium-sized enterprises SMEs and start-ups**.

6 Governance and Implementation

Governance

A governance system is established at both the Union and National level for the purpose of directing, controlling and executing this Regulation

Union Level

At Union level, the "**European Artificial Intelligence Board**" (the 'Board') is established for the purpose of **providing advice and assistance to the EC**. In order to coordinate, contribute and assist with matters covered by this Regulation.

Structure of the Board

The Board is expected to be composed of the **national supervisory authorities, and the European Data Protection Supervisor.**

It should adopt its rules of procedure by a **simple majority of its members**, following the consent of the EC. The rules of procedure shall also contain the **operational aspects related to the execution of the Board's tasks**.

The Board is expected to be chaired by the EC, which will provide administrative and analytical support for the Board's activities pursuant to this Regulation.

Tasks of the Board

Collect and share **expertise and best practices** among Member States; **contribute to uniform administrative practices** in the Member States and **issue opinions, recommendations or written contributions on matters** related to the application of this Regulation.

The **European Data Protection Supervisor** will act as the competent authority for the **supervision** of the Union institutions, agencies and bodies when they fall **within the scope of this regulation**.

National Level

The **competent national authorities** are expected to be **established or designated** by each Member State for the purpose of **ensuring the implementation and enforcement** of this Regulation. Such authorities will be organized in such a way as to ensure the objectivity and impartiality of their activities and tasks.

Each Member State shall designate a national supervisory authority from among the NCAs, acting as notifying authority and **market surveillance authority.** NCAs may provide **guidance and advice on the implementation of this Regulation**, including to small-scale providers.

6 Governance and Implementation

Implementation

The Regulation establishes the monitoring and reporting obligations for providers of AI systems with regard to post-market monitoring and reporting and investigating on AI-related incidents and malfunctioning controlled by Market surveillance authorities

EU Database

To **facilitate the monitoring work of the EC** and national authorities, an EU-wide database is stablished **for stand-alone high-risk AI systems with mainly fundamental rights implications**. The database will be operated by the EC and **provided with data by the providers of the AI systems,** who will be required to register their systems before placing them on the market or otherwise putting them into service.

Post-Marketing

Post-Market Monitoring	Providers are expected to **establish and document a post-market monitoring system** proportionate to the nature of the AI technologies and the risks of the high-risk AI system. This system should actively and systematically **collect, document and analyze relevant data provided by users** on the **performance of high-risk AI systems** throughout their lifetime, and **allow the provider to evaluate the continuous compliance with the high-risk AI systems requirements**. The EC is expected to **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.
Reporting incidents and malfunctions	**Providers of high-risk AI systems** placed on the EU market should **report any serious incident or any malfunctioning of those systems** which constitutes a breach of obligations under EU law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred.
Enforcement	**Market surveillance authorities would control the market and investigate compliance with the obligations and requirements for all high-risk AI systems already placed on the market**.

7 Codes of conduct
Main aspects

Codes of conduct, which aim to encourage providers of non-high-risk AI systems to apply voluntarily the mandatory requirements for high-risk AI systems

Providers of non-high-risk AI systems

- Providers of non-high-risk AI systems may create and implement the codes of conduct themselves. Codes of conduct may include **voluntary commitments related to**:
  - Environmental sustainability.
  - Accessibility for persons with disability.
  - Stakeholders' participation in the design and development of AI systems.
  - Diversity of development teams.

- The **EC and the Member States** shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems.
- Codes of conduct may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.
- The **EC and the Board** shall take into account the specific interests and needs of the **small-scale providers and start-ups** when encouraging and facilitating the drawing up of codes of conduct.