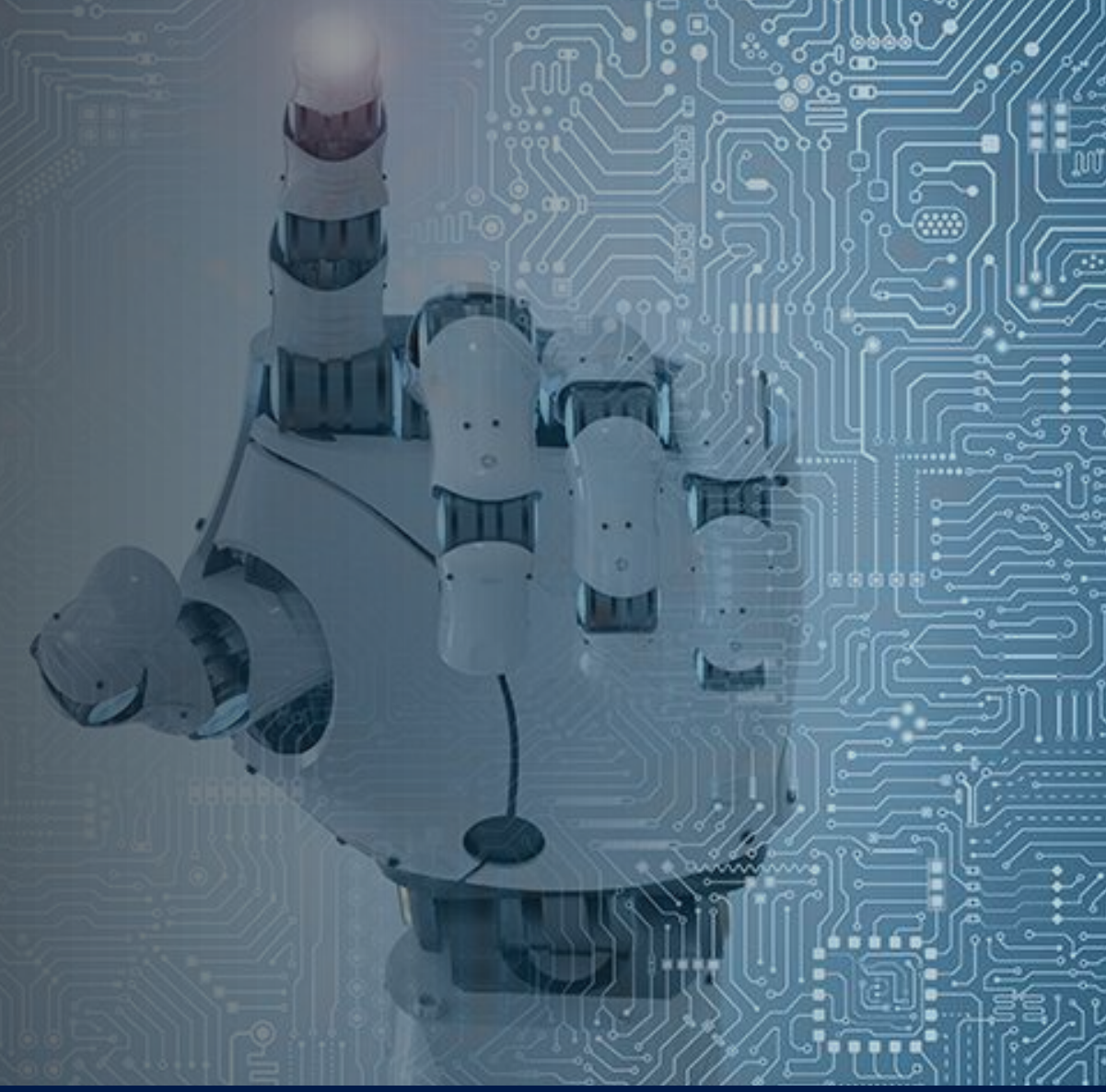
Artificial Intelligence Act

European AI Regulation (Council adopted version)



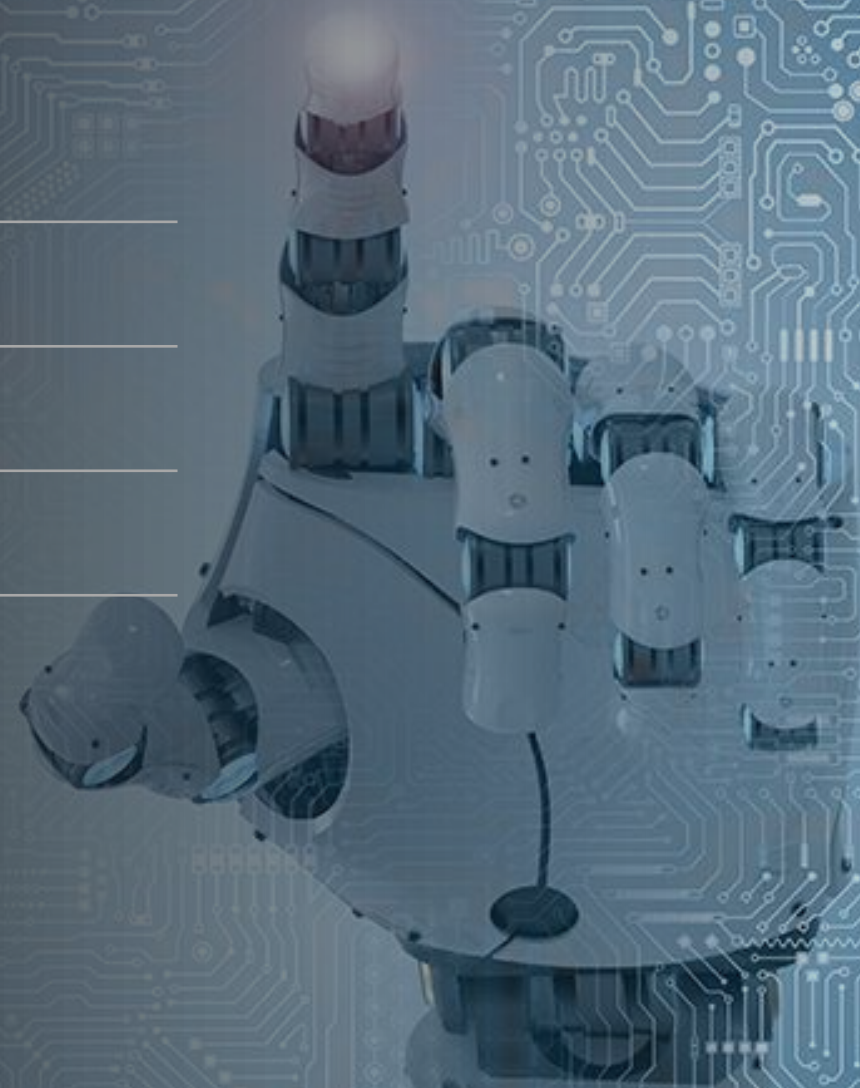
© Management Solutions 2024. All rights reserved

General Overview

AI Systems

Regulatory Sandboxes

Governance



1 General Overview
Executive summary

On May 2024, the Council approved the AI Act, bringing the legislative process to an end

Context

- The AI Act comes in response to the growing application and potential of AI systems in various sectors, along with the need to address the potential risks and harms that these systems may cause to public interests, health, safety and fundamental rights protected by the EU.
- The proposal was presented by the EC in 2021, followed by opinions from various bodies such as the ECB and the European Economic and Social Committee.
- After the EP's adoption at first reading in March 2024, the Council has approved the text with minor changes over the EP's version.

Objective

- The main objective of the AI Act is to improve the functioning of the internal market by establishing a uniform legal framework for the development, marketing, use and servicing of AI systems in the EU.
- This is done with the intention of promoting the adoption of **human-centered and reliable AI**, while ensuring a high level of protection against the harmful effects of AI systems and supporting innovation.

Next Steps

- The text will enter into force 20 days after its publication in the OJEU.
- It will be fully applicable **24 months after its entry into force**, except bans on prohibited practices, which will apply **6 months after**; codes of practice, **9 months after**, general-purpose AI rules including governance, **12 months after**, and obligations for high-risk systems, **36 months after**.
- The Commission shall develop **guidelines** on the **practical implementation** of this Regulation (art. 96).

Contents

AI Systems and risk-based classification	• AI System definition and establishment of a risk-based classification (unacceptable, high-risk and non-high risk)
Regulatory Sandboxes	• The EC encouraging to set up regulatory sandboxes and setting a basic framework in terms of governance, supervision and liability, in order to keep a legal framework that is sustainable over time and innovation-friendly
Governance	• Establishing a governance system at both the Union and National level for the purpose of directing, controlling and executing this Regulation

Access to Document

© Management Solutions 2024. All rights reserved

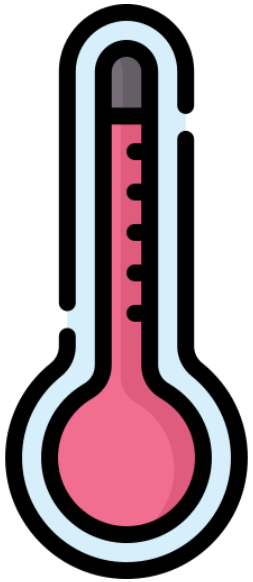
2 AI Systems
Definition and classification

AI systems are defined, and a risk-based classification is established, including risk categories (unacceptable, high-risk, and minimal risk)

Definition

- **AI system** is a **machine-based system** designed to **operate with varying levels of autonomy**, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, **infers**, from the input it receives, **how to generate outputs** such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Risk based classification



Unacceptable Risk

- AI applications that threaten citizens' rights, such as biometric categorization systems based on sensitive characteristics, non-selective tracking of facial images from the Internet or closed-circuit television (CCTV) recordings for facial recognition databases, cognitive manipulation and social scoring. The AI Act prohibits these unacceptable risk AI systems.

High Risk

- AI used in biometrics, critical infrastructure (e.g. road traffic or in the supply of water) education and vocational training (e.g. to determine access or admissions, to evaluate learning outcomes), employment, workers management 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, and administration of justice and democratic processes (e.g. in dispute resolution). Citizens will have the right to lodge complaints about AI systems and to receive explanations of decisions based on high-risk AI systems that affect their rights.

Minimal Risk

- An AI system is considered to be of minimal risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.

© Management Solutions 2024. All rights reserved

2 AI Systems
Unacceptable Risk

The regulation prohibits certain AI practices classified as unacceptable risks as some cases of placing on the market, putting into service or use of AI and some remote biometric identification systems

Some cases of placing on the market, putting into service or use of AI (art. 5)

- Practices 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 significant harm.
- Practices 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.
- Practices that categorise natural persons according to sensitive or protected attributes or characteristics or based on the inference of those attributes or characteristics.
- Practices 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.
- Practices for **making risk assessments of natural persons or groups thereof** in order to assess the risk of a natural person for offending or reoffending.
- Practices that **create or expand facial recognition databases** through the untargeted scraping of facial images from the internet.
- Practices to **infer emotions of a natural person** in the areas of law enforcement, border management, in workplace and education institutions.

Remote biometric identification systems (art. 5)

- Used of "real-time" **remote biometric identification systems in public spaces.**
- Used for the analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, unless they are subject to a pre-judicial authorisation in accordance with Union law.

© Management Solutions 2024. All rights reserved

2 AI Systems

High-Risk: Legal requirements and obligations for providers

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 (Art. 9)

- 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 (Art. 16)

- **Ensure that their high-risk AI systems are compliant with the legal requirements.**
- Indicate their name, registered trade name or registered trade-mark, and their address and contact information on the high-risk AI system.
- Have a **quality management** system in place.
- Keep 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.
- Draw up an EU declaration of conformity.
- Affix the EC marking to the high-risk AI system or on its packaging or its accompanying documentation, to indicate conformity with this Regulation.
- Comply with the **registration obligations.**
- Take the **necessary corrective actions**, if the high-risk AI system is not in conformity with the legal requirements.
- Upon a reasoned request of a national competent authority (NCA), demonstrate the conformity of the high-risk AI system.
- Ensure that the high-risk AI system complies with accessibility requirements.

© Management Solutions 2024. All rights reserved

2 AI Systems
High-Risk: 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

Assessment procedure key elements

Harmonized standards (art. 40)

- Aim to minimise the burden for economic operators and notified bodies. **High-risk AI systems** which are in **conformity with harmonized standards** or parts thereof shall be presumed to be **in conformity with the legal requirements** for high-risk AI systems.

Conformity assessment (art. 43)

- The provider shall follow the **conformity assessment procedure** based on **internal control** or the one based on the **assessment of the quality management system** of the technical documentation, with the involvement of a notified body.

Certificates (art. 44)

- **Certificates** issued by notified bodies shall be **drawn-up in an official Union language** and will be valid up to **five years.**

Registration (art. 49)

- Before placing on the market or putting into service a high-risk AI system referred, the provider shall register that system in the **EU database**, as well as deployers who are public authorities or Union institutions, and deployers who are undertakings designated as a gatekeeper.

Notification framework

Notifying authorities (art. 28)

- Designated or established by each Member State.
- **Responsible for setting up and carrying out the necessary procedures** for the assessment, designation and notification of conformity assessment bodies and for their monitoring.
- They shall **not offer or provide any activities that conformity assessment bodies perform or any consultancy services** on a commercial or competitive basis.

Notification procedure (art. 30)

- Notifying authorities shall notify the EC and the other Member State using the **electronic notification** tool developed and managed by the EC of each conformity assessment body.
- **Full details of the conformity assessment activities** shall be included, together with the conformity assessment module, the AI technologies concerned and the relevant attestation of competence.

Notifying bodies (art. 31)

- 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 as well as the minimum cybersecurity requirements set out for public administration entities.
- **Independent of the provider** of a high-risk AI system in relation to which it performs conformity assessment activities.

© Management Solutions 2024. All rights reserved

2 AI Systems
High-Risk: Monitoring and reporting obligations

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 (Art. 71)

- To **facilitate the monitoring work of the EC** and national authorities, an EU-wide database is stablished **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 (Art. 72)

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. 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 and, where deployers have identified a serious incident, of high-risk AI systems** placed on the EU market should **report any serious incident** of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the national supervisory authority 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.

© Management Solutions 2024. All rights reserved

2 AI Systems
Non-High Risk

Non-high risk AI systems providers are encouraged to implement codes of conduct, which aim to apply voluntarily the mandatory requirements for high-risk AI systems

Codes of conduct (art. 95)

- 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.

Transparency obligations will apply for systems that (Art. 50)

- Systems providers that interact with humans, 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**.

- Systems used to detect emotions or determine association with (social) categories based on biometric data, shall inform of the operation of the system the natural persons exposed thereto.

- Systems that generate or manipulate content (deep fakes), 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 to the systems that interact with **humans shall not apply** where the use is authorised by law to detect, prevent, investigate and prosecute **criminal offences**.

© Management Solutions 2024. All rights reserved

3 Regulatory Sandboxes
Basic framework

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

Member State shall establish at least one **AI regulatory sandbox** at national level fosters innovation and 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. Additional AI regulatory sandboxes at regional or local levels may also be established:

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, democracy and rule of law, health and safety or the environment **identified during the development and testing** of such systems shall result in immediate **mitigation.** CAs shall have the power to temporarily or permanently suspend the testing process, or participation in the sandbox if no effective mitigation is possible and inform the AI office of such decision.

Any **member state** establishing AI regulatory sandboxes is expected to **cooperate under the framework of the European Artificial Intelligence Board** through **annual reports,** starting one year after the establishment of the sandbox and then every year until its termination and a final report. Those reports shall provide information on the progress and results of the implementation of those sandboxes including experience obtained in all areas. Those annual reports or abstracts thereof shall be made available to the public, online.

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

© Management Solutions 2024. All rights reserved

4 Governance
Union level and national level

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

Union Level (Arts. 65,66)

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

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

- Monitor and ensure the effective and consistent application of this Regulation.
- Serve as a mediator in discussions about serious disagreements regarding the application of the Regulation.
- Contribute to the effective cooperation with the competent authorities of third countries and with international organisations.
- Collect and share expertise and best practices among Member State.

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 (Art. 70)

The **competent national authorities** are expected to be **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.

Member States shall make publicly available and communicate to the AI Office and the Commission the national supervisory authority and information on how it can be contacted.

© Management Solutions 2024. All rights reserved

ManagementSolutions

Making things happen

International *One Firm*

Multiscope Team

Best practice *know-how*

Proven Experience

Maximum Commitment

Javier Calvo Martín
Partner at Management Solutions
Javier.calvo.martin@managementsolutions.com

Manuel Ángel Guzmán
Partner at Management Solutions
Manuel.guzman@managementsolutions.com

Marta Hierro
Partner at Management Solutions
Marta.Hierro@msspain.com

© Management Solutions, 2024

All rights reserved. Cannot be reproduced, distributed, publicly disclosed or transformed, whether totally or partially, free of charge or at no cost, in any way or by any means, without the express written authorization of Management Solutions.

The information contained in this publication is merely to be used as a guideline, is provided for general information purposes and is not intended to be used in lieu of consulting with our professionals. Management Solutions is not liable for any use that third parties may make of this information. The use of this material is not permitted without the express authorization of Management Solutions.

For more information please visit

www.managementsolutions.com

Or follow us at: