

# The Eu Parliament approves the European Regulation on Artificial Intelligence: the implications for businesses

## I Approval and timing of application

On March 13, the European Parliament voted, by a large majority, in favour of the **proposal for a EU Regulation** laying down harmonised rules on Artificial Intelligence ("**Regulation**"), also known as the Artificial Intelligence Act ("**AI Act**").

Although the legislative process is not yet completely finalised, as it is still subject to final legal-linguistic scrutiny and formal approval by the Council, it seems likely that it will be definitively adopted by the summer.

The regulation represents the world's **first comprehensive piece of legislation on artificial intelligence** and will enter into force 20 days after its publication in the Official Journal of the Union.

The AI Act will thus become **directly applicable two years after its entry into force, with the exception of some specific provisions**:

- **The provisions on prohibited artificial intelligence practices** will be applicable **six months** after entry into force;
- The provisions **on codes of conduct** will become applicable **nine months** after entry into force;
- The provisions related to **General Purpose AI ("GPAI")** models will become applicable **twelve months** after entry into force;
- The obligations for **high-risk systems** will become applicable **thirty-six months** after entry into force.



Source: <https://futurium.ec.europa.eu/fi/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act?language=en>

However, European and non-European economic operators will have the option – on a voluntary basis – to anticipate the application of the AI Act’s rules before the legal deadlines mentioned above. This can be achieved by joining the so-called “**AI Pact**”, an initiative led by the European Commission, which aims to foster compliance with the new rules **as early as this year**, through the adoption of commitment statements and implementation plans.

## II Scope and main provisions of the new Regulation

The AI Act aims to both foster and ensure that AI systems placed on the **EU single market** are safe and robust, ensuring respect of fundamental rights of individuals, democratic principles, and environmental sustainability.

In light of the upcoming publication of the Regulation, a summary overview of the main provisions of the new regulation is outlined below.

**(1) Scope.** The definition of “AI systems” adopted by the Regulation is aligned with **the one most recently proposed by the OECD**. It therefore includes those systems designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment which, for explicit or implicit objectives, infer from the inputs received how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. This definition **excludes software of a less complex nature, programming approaches** and systems that are based on the rules defined solely by natural persons to automatically execute operations. AI systems used

for **military, defense, research and innovation purposes, or for non-professional uses** (and, under certain conditions, those provided under open-source licenses) are likewise excluded.

From a subjective standpoint, the **extra-territorial scope** of the new discipline is of particular importance: the forthcoming AI Act will in fact apply **also** to **non-EU players and organizations** having establishment within the Union or offering goods or services in the Union market (even in the absence of an establishment in the Union).

**(2) Classification of AI systems: risk-based approach.** The AI Act adopts a risk-based approach, **firstly prohibiting certain practices whose level of risk is deemed unacceptable**. The prohibition covers practices which have a significant potential to manipulate persons through subliminal techniques, **social scoring, emotion recognition systems** in the context of employment or education or for the exploitation of vulnerabilities of individuals and vulnerable groups.

Notwithstanding these prohibitions, the architecture of the AI Act distinguishes:

**(i) High-risk AI systems:** such as systems employed in medical devices, vehicles, recruiting processes, critical infrastructures, or access to essential public or private services (e.g., health services, access to credit). Such systems will have to comply with specific obligations and requirements in terms of risk & quality management, data governance, transparency and human oversight, as well as accuracy, robustness, and cybersecurity. Moreover, high-risk systems which are required to be registered in a public EU database for high-risk AI systems will only be allowed to be placed on the EU market after conducting a fundamental rights impact assessment and successfully undergoing a conformity assessment procedure.

**(ii) Minimal-risk AI systems:** those that are not included among the unacceptable or high-risk systems, in relation to which the discipline does not introduce new obligations – except for the cases under item *(iii)* below and save in any case the possibility for companies to adhere to voluntary codes of conduct.

**(iii) AI systems subject to specific transparency risks:** in case of AI systems intended to directly interact with natural persons, operators will have to comply with significantly less onerous obligations, mostly of an informative nature (e.g., with respect to the use of chatbots, users shall be made aware that they are interacting with a machine, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use).

**(3) General-purpose AI models (GPAIs).** One of the most contentious issues during the AI Act negotiations revolved around the **discipline applicable to so-called GPAIs**, including Large Generative Models that can be used for various distinct purposes, such as video, image and text generation (e.g., ChatGPT, Gemini, Midjourney, etc.). Concerning such systems, the new Regulation sets forth **certain cross-cutting obligations applicable to all GPAIs. These obligations** include compliance with European **copyright** law and documentary requirements such as providing the public with a detailed summary of the **content used for AI training**. In addition, criteria have been introduced to assess whether a given GPAI poses **systemic risks<sup>1</sup>**, **in which case the relevant GPAI will be subject to further requirements** in terms of model evaluation, systemic risk assessment and mitigation, adversarial testing, cybersecurity, energy efficiency, and reporting of major incident to the European Commission.

**(4) Regulatory sandboxes.** The Regulation expressly provides for an obligation on Member States (alone or jointly) to set up **regulatory sandbox** initiatives, in order to foster the development of AI systems in a “protected environment” – particularly by European SMEs – before their introduction to the market. This is a point on which members of the European Parliament have placed particular emphasis in order to encourage the emergence of European players.

**(5) Governance.** The Regulation provides for the establishment of an **AI Board**, which will serve as an advisory body to the European Commission.

---

<sup>1</sup>According to the text of the Regulation, the classification of GPAI models as systems involving systemic risks will initially depend on the calculation capacity of such systems: based on a quantitative threshold of the cumulative amount of calculation used for training and measured in floating point operations per second (FLOPs) - or on an individual designation decision of the Commission. The initial threshold of FLOPs is set at  $10^{25}$  FLOPs and the Commission will be obliged to adapt this threshold in the light of evolving technological developments .

An **AI Office** has already been set up within the European Commission - by decision dated 24 January 2024 - which will oversee, among other things, the implementation of the provisions for GPAI models. In addition, an **Advisory Forum** composed of stakeholders representing industry, civil society, and academia, with advisory functions, and a **Scientific Panel** of independent experts, tasked with supporting the implementation and enforcement of the provisions applicable to GPAI models, will be established. Finally, each member state is called upon to identify the competent national enforcement authority for the AI Act.

**(6) Non-discrimination.** The Regulation intends to ensure compliance with non-discrimination principles (including gender equality) by introducing specific requirements aimed at minimising the risk of algorithmic discrimination in relation to the design and quality of the data sets used for the development of AI systems. AI systems should be developed in such a way as to avoid discriminatory effects and unfair bias, and to support diversity, nondiscrimination, and equity.

**(7) Penalties.** Infringements of the AI Act will lead to fines, which -following an approach similar to that of the GDPR- may be determined on the basis of the total worldwide annual turnover of the preceding financial year of the company to which the violation is attributed. Namely, monetary penalties are provided for up to a maximum of:

**(i) -€35 million or 7% of the total worldwide annual turnover** (whichever is higher) for infringements on prohibited practices;

**(ii) €15 million or 3% of the total worldwide annual turnover** (whichever is higher) for noncompliance with any of the other requirements or obligations of the Regulation, including infringement of the rules on general-purpose AI models; and

**(iii) €7.5 million or 1% of the total worldwide annual turnover** (whichever is higher) for the supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request.

In case of SMEs, including start-ups, each fine referred to above shall be up to the percentages or amount referred to the relevant violation, whichever of the two is lower.

## III Implications for economic operators

Although the actual implementation of the Regulation is subject to the timeline set forth in paragraph 1. above, it is appropriate to outline as of now the coordinates of the AI compliance strategy. This includes identifying key actions for the prospective and progressive adoption of the safeguards required by the AI Act.

- **Action Plans.** As compliance with the new rules will take time, it is advisable for economic operators to begin preparing compliance roadmaps, also in light of the fact that some of the obligations under the AI Act will become applicable before the general deadline of 24 months after approval.
- **Mapping.** Implementing compliance actions involves carrying out preliminary assessments related, among others, to the number and characteristics of the AI systems that are intended to be developed, marketed and/or adopted, the intended uses of such systems (including their related risks), and the role played by the economic operator in relation to them. In this regard, for example, it will be crucial to determine whether the AI systems under consideration can be deemed to fall within the prohibitions , or those considered “high-risk,” or “discriminatory” scenarios, circumstances from which important compliance requirements may arise.
- **Governance models.** The adoption and use of AI systems should be adequately reflected in the structuring of governance models aimed at ensuring a clear allocation of related decision-making and management powers within the entity’s organization, with a view to ensure accountability (where appropriate, also through the involvement of external experts).
- **Policy and Procedures.** Without prejudice to the obligations under the AI Act, economic operators are encouraged to verify their compliance initiatives also in light of industry best practices and general principles on the responsible use of AI systems. These principles can be derived from documents adopted by supranational bodies, including the “Ethics

guidelines for trustworthy AI” adopted within the EU<sup>1</sup>, the “AI Principles” adopted by the OECD<sup>2</sup> , or the proposed “Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law<sup>3</sup>” of the Council of Europe. Additionally, virtuous models adopted by major market players may be considered as well. a first review of policies and procedures may extend to the management of procurement by third-party vendors, as well as to audit activities addressing the vendors themselves, also to encourage ethical and non-discriminatory use of AI.

- **Documentation.** Whether it concerns preliminary evaluations regarding the implementation of possible AI use cases or the adoption of AI tools, starting with limited scopes and then becoming increasingly ambitious, documenting all evaluations and choices made in relation to AI systems is a well-established best-practice. For example, assessments related to the risks of using AI systems for individual’s fundamental rights are relevant to this end.

- **Ongoing training.** The technical skills required for the adoption of AI systems and the risks associated with their use make it appropriate to structure targeted and documentable training paths for all subjects who, in different capacities, are or will be involved in implementing such systems.

- **Relationship with other legislation.** The development and adoption of AI systems are subject to the application of other already existing regulations, such as the GDPR. In this regard, economic operators are encouraged to evaluate solutions and processes allowing for the efficient management of compliance obligations and risks from a perspective of integrated compliance.

- **Pact for AI.** The early compliance instrument envisaged by the European Commission represents an opportunity for economic operators who, by structuring a gradual compliance plan, would benefit from the

---

<sup>2</sup>Available at the following link: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

<sup>3</sup>Available at the following link: <https://oecd.ai/en/ai-principles>.

<sup>4</sup>Available at the following link: <https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043>.

advantage of **(i)** already having initiated the first phases of the adaptation path and compliance strategy when the AI Act when the AI Act becomes applicable, **(ii)** strengthening their competitive position on the market, as well as **(iii)** increasing the trust relationship with their customers and/or stakeholders. The Commission has already established a dedicated online platform to collect expressions of interest in the project.

---

## Contacts

### **Pierluigi Perri**

Of Counsel – Chiomenti  
Data Protection & Cybersecurity  
T. +39.02.721.571  
[pierluigi.perri@chiomenti.net](mailto:pierluigi.perri@chiomenti.net)

### **Marilena Hyeraci**

Of Counsel – Chiomenti  
Data Protection & Cybersecurity  
T. +39. 02.721.571  
[marilena.hyeraci@chiomenti.net](mailto:marilena.hyeraci@chiomenti.net)

### **Matteo Leffi**

Associate – Chiomenti  
Data Protection & Cybersecurity  
T. +39. 02 72157 717  
[matteo.leffi@chiomenti.net](mailto:matteo.leffi@chiomenti.net)

### **Tommaso Bratina**

Trainee – Chiomenti  
Data Protection & Cybersecurity  
T. +39. 02 72157 717  
[tommaso.bratina@chiomenti.net](mailto:tommaso.bratina@chiomenti.net)