KLEYR GRASSO

26 January 2026

ARTIFICIAL INTELLIGENCE

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, and the Luxembourg draft bill No. 8476.

The European regulation on artificial intelligence (AI Act – Regulation (EU) 2024/1689) has now been adopted. For businesses, the challenge is very concrete: identify your role (provider, deployer, etc.), determine the level of risk, and organise compliance accordingly.

📌 **Three key takeaways**

☑ **Role**: where do you sit in the value chain (provider, deployer, importer, distributor, etc.)?

⚖ **Risk**: what is the system's level of risk in light of its purpose and its context of use?

🗂 **Traceability**: what governance and documentation measures should be put in place to demonstrate compliance and manage liability?

This first introductory note, deliberately educational in nature, aims to explain the main principles of the AI Regulation and the first practical implications, with a focus on implementation in Luxembourg.

1. BACKGROUND – UNDERSTANDING THE AI ACT: WHERE DOES IT COME FROM AND WHAT IS IT FOR?

The AI Act is the common name given to Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending several existing regulations and directives (the **AI Act**).

It is an EU regulation, i.e. a legal act that is directly applicable in all EU Member States, without any need for transposition into national law. The obligations it sets out therefore apply directly to the relevant stakeholders, subject to the national implementing measures provided for by the text, in particular regarding the competent authorities, supervisory and enforcement mechanisms, and the sanctions regime.

The purpose of the AI Act is to govern the development, placing on the market and use of artificial intelligence systems, based on the risks those systems may present. To that end, it does not proceed in an abstract manner: it adopts a specific legal definition of artificial intelligence, which determines the scope of its application as a whole.

Accordingly, the AI Act defines an "*artificial intelligence system*" as "*a machine-based system that is designed to operate with varying levels of autonomy and 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.*"

This definition is deliberately broad and technologically neutral. It does not target a specific technology, but rather a function: a system's ability to produce, in an automated manner, outputs that have an impact on its environment. As a result, many software tools used in a professional context may fall within the scope of the AI Act, even where they are not presented as "*artificial intelligence*" in the everyday sense of the term.

2. WHY THE AI ACT?

The adoption of the AI Act takes place against a backdrop of profound change in digital uses. As the opening recitals of the AI Act recall, artificial intelligence is no longer an experimental or marginal technology. It is now embedded in many tools and processes that directly shape economic, social and professional life.

Artificial intelligence systems are now used to automate or support decisions across a wide range of areas, such as recruitment and human resources management, access to essential services, the assessment of individual situations, and decision support in sensitive environments. These uses can have very tangible effects on the persons concerned, whether in terms of access to a job, a service, or a right.

At the same time, the EU legislator does not deny the significant benefits associated with the development of artificial intelligence. Recital (4) of the AI Act expressly notes that artificial intelligence is a fast evolving family of technologies that contributes to a wide array of economic, environmental and societal benefits, and explains that, by improving prediction, optimising operations and resource allocation and personalising digital solutions, the use of artificial intelligence can provide key competitive advantages and support socially and environmentally beneficial outcomes.

In that regard, pursuant to the AI Act, artificial intelligence systems can bring significant benefits to individuals, businesses and society as a whole, notably by improving predictions, optimising operations and resource allocation, and personalising digital solutions across many economic and social sectors. They can also contribute to objectives of general interest, such as better healthcare, disease prevention, enhanced security and the promotion of environmental sustainability.

However, it is important not to overlook the specific risks that certain uses of artificial intelligence may pose to fundamental rights and the Union's values. Those risks relate in particular to the opacity of certain automated decisions, the difficulty of understanding or challenging the outputs produced by an artificial intelligence system, biases that may affect data or models, and issues of system security and reliability. In that respect, Recital (5) of the AI Act recalls that "[s]*uch harm might be material or immaterial, including physical, psychological, societal or economic harm*."

Before the adoption of the AI Act, these issues were addressed through general rules under existing law, such as data protection, consumer law or product safety rules. While those frameworks remain applicable, they were not designed to respond specifically to the distinctive features of artificial intelligence. This situation created a degree of legal uncertainty, both for affected persons and for businesses, and entailed a risk of divergent approaches across Member States.

In response to this, the European Union has chosen to intervene through a specific, horizontal and harmonised legal framework, directly applicable across all Member States. As Recital (1) of the AI Act states, that framework aims to "*improve the functioning of the internal market*", to promote the uptake of human centric and trustworthy artificial intelligence, and to ensure a high level of protection of health, safety, fundamental rights "*enshrined in the Charter of Fundamental Rights of the European Union, including democracy, the rule of law and environmental protection*", while supporting innovation.

It is in this vein that the AI Act adopts a risk-based approach, distinguishing artificial intelligence systems according to the level of risk they are likely to pose and, consequently, the impact they may have on health, safety and fundamental rights. This architecture, which is the guiding thread of the AI Act, makes it possible to regulate the most sensitive uses more strictly, while maintaining a lighter framework for low-risk applications.

3. HORIZONTAL SCOPE OF THE AI ACT AND TARGETED STAKEHOLDERS

One of the AI Act's structuring features is its horizontal nature: it is not limited to a single sector (banking, healthcare, insurance, HR, etc.), but establishes a uniform legal framework that applies, across the board, to the development, placing on the market, putting into service and use of artificial intelligence systems in the Union.

This approach is reflected first in a very broad personal and territorial scope. The AI Act applies not only to actors established in the Union, but also to certain actors established outside the Union where (i) they place artificial intelligence systems on the Union market or put them into service in the Union, or (ii) the output produced by the artificial intelligence system is used in the Union.

Beyond territorial scope, the AI Act then reasons in terms of "*operators*", understood as the key participants in the artificial intelligence value chain. This is a structuring approach: obligations vary depending on the role performed, and a single actor may combine multiple roles. In that respect, the AI Act explicitly targets providers, deployers, importers, distributors, authorised representatives (for providers not established in the Union) and, in certain cases, product manufacturers that market an AI system together with their product and under their own brand.

The AI Act defines these roles functionally:

- "*provider*" means "a […] *person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark",* whether for payment or free of charge.
- "*deployer*" means "*a* […] *person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity*".
- "*authorised representative*" means "*a* […] *person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established"* by this AI Act.
- "*importer*" means "*a* […] *person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country*".
- "*distributor*" means "*a* […] *person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market*".

The AI Act groups these various stakeholders under the concept of "*operator*" which is defined as "*a provider, product manufacturer, deployer, authorised representative, importer or distributor*".

In practice, the "*operator*" approach adopted by the AI Act creates a compliance prerequisite: for each relevant artificial intelligence system, the organisation must determine the role it occupies in the value chain (provider, deployer, importer, distributor, etc.). This classification is not merely theoretical, as it directly determines the nature and intensity of the applicable obligations.

One point warrants particular attention: the AI Act provides for situations in which an actor that was not initially the provider may be legally treated as such, in particular for high-risk artificial intelligence systems—notably where an actor places a system on the market under its own name or trademark, makes a substantial modification, or changes the intended purpose in a way that brings the system within the high-risk regime.

In other words, the issue is not merely terminological: it is one of compliance and liability. This justifies, from the outset, putting in place minimal and traceable internal governance (allocation of responsibilities, appropriate contractual clauses, change-control processes, and validation prior to placing on the market or putting into service).

4. A RISK-BASED APPROACH: THE AI ACT "PYRAMID"

The AI Act is built around a guiding idea: not all artificial intelligence systems present the same level of risk, and it is neither relevant nor effective to subject all uses to the same obligations. The AI Act therefore adopts a graduated approach, based on the level of risk associated with an artificial intelligence system and, where applicable, with the use made of it, in order to impose requirements that are proportionate to the potential impact on health, safety and fundamental rights.

In concrete terms, the logic is as follows: the higher the risk, the more demanding the framework becomes. The AI Act thus combines (i) targeted prohibitions of certain practices deemed incompatible with the Union's values, (ii) a strengthened regime for so-called high-risk systems, and (iii) more limited obligations—particularly in terms of transparency—for certain specified systems or uses.

This architecture is not merely theoretical: it structures compliance in practice. For a company, the first question is therefore not "do we use AI?", but rather: "what level of risk is attached to the system in question, in light of its purpose and its context of use?" The stakes are significant, because the system's classification directly determines the scope of the applicable obligations, in particular where the system qualifies as a high-risk artificial intelligence system.

Finally, one decisive point should be emphasised: the assessment of risk does not depend solely on technological sophistication, but above all on the function performed and the effects the system is likely to produce. The same tool may therefore fall under different regimes depending on the domain, the intended purpose and the specific conditions under which it is deployed.

Without going into detail here—which will be the subject of upcoming newsletters—the AI Act establishes a graduated set of requirements. In broad terms, it distinguishes (i) prohibited practices (so-called "*unacceptable*" risk), (ii) a central core of "high-risk" systems subject to an enhanced regime, and (iii) transparency obligations applicable in certain situations, while "*low-risk*" systems fall within a significantly lighter framework.

- **"*Unacceptable-risk*" practices:** certain practices are considered incompatible with the Union's values and are therefore prohibited. The AI Act sets out a list of prohibited practices (with strictly framed exceptions in certain cases), which may not be placed on the market, put into service or used in the Union.

- **"*High-risk*" systems:** the core of the framework concerns systems classified as "*high-risk*". The key point—particularly important for businesses—is that this "*high-risk*" classification does not depend solely on technological sophistication: it stems above all from the intended purpose and the context of use, i.e. the system's capacity to significantly affect health, safety or fundamental rights. In some cases, "*high-risk*" status also results from the integration of an artificial intelligence system into products already covered by harmonised legislation. These systems are subject to enhanced and structured requirements (governance, documentation, data quality, human oversight, security, etc.), which will be addressed in a dedicated instalment of this series.

- **Transparency obligations:** irrespective of "*high-risk*" status, the AI Act provides for transparency obligations in specific situations: where a person interacts with certain artificial intelligence systems, or where content is generated or manipulated by artificial intelligence in the cases covered, the public must be informed in accordance with the applicable requirements.

- **"*Low- or minimal-risk*" systems:** conversely, a large share of everyday uses—where they do not raise a significant risk in light of the objectives protected by the AI Act—fall within a significantly lighter framework. It is precisely this gradation that allows the AI Act to be presented as a proportionate regulatory instrument, rather than a general prohibition.

In practice, this "pyramid" calls for a method: identify the role, then assess the system's risk level, in order to determine the applicable set of requirements and document that assessment, since it is a condition of compliance.

5. THE AI ACT: A PRACTICAL GUIDE FOR BUSINESSES

Beyond the concepts, the AI Act requires companies to follow a highly pragmatic approach: identify whether, where and how artificial intelligence is used in their activities, then determine the applicable regime and organise compliance accordingly. The issue is therefore not merely technological: it is first and foremost legal, organisational and contractual, since obligations vary depending on (i) the role played in the value chain (provider, deployer, etc.) and (ii) the level of risk associated with the system and its use.

In practice, three questions structure the analysis and provide a roadmap through the text:

1. What is our role in relation to the artificial intelligence system concerned (and do we combine several roles)?

2. What level of risk is associated with the AI system, in light of its purpose and its concrete context of use?

3. What governance, control and documentation measures must be put in place to demonstrate compliance and manage the associated liability?

6. A DELIBERATELY LIMITED SCOPE

Despite its horizontal ambition and broad territorial reach, the AI Act provides for a number of exclusions and coordination clauses. The objective is twofold: (i) to avoid the AI Act encroaching on areas that do not fall within EU law or that relate to essential sovereign functions, and (ii) to preserve, within a framed approach, research and innovation, while ensuring consistency with other applicable legal frameworks.

- **Exclusions relating to national security, defence and military matters.**

  The AI Act clarifies that it does not apply to areas falling outside the scope of Union law and that it "*shall not, in any event, affect the competences of the Member States concerning national security*". It further excludes artificial intelligence systems that are "*placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes*", including where the output produced by those systems (their "outputs", such as predictions, recommendations or decisions) is used in the Union exclusively for those purposes.

- **An exception for certain uses by third-country authorities in the context of law enforcement and judicial cooperation.**

  The AI Act also excludes its application "*to public authorities in a third country*" and "*to international organisations*" where those authorities or organisations "*use artificial intelligence systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States*", provided that the relevant third country or international organisation "*provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals*."

- **"Innovation" exclusions: research and pre-market activities — with an important limitation.**

  The AI Act does not apply to artificial intelligence systems (or general-purpose artificial intelligence models) specifically developed and put into service for the sole purpose of scientific research and development, nor to their output. Likewise, it excludes research, testing or development activity regarding artificial intelligence systems or artificial intelligence models prior to their being placed on the market or put into service, while specifying that testing in real world conditions is not covered by that exclusion.

- **Strictly personal use: a targeted exclusion from deployer obligations.**

  The AI Act provides that the obligations applicable to deployers do not apply where the deployer is a natural person using an artificial intelligence system in the course of a strictly personal non-professional activity.

- **Free and open-source software: an encouraging approach, but not an absolute exemption.**

  The AI Act states that it does not apply to artificial intelligence systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk systems, or unless they fall under the specific regimes for prohibited practices or for certain transparency obligations.

- **Coordination clauses: the AI Act does not replace other legal instruments.**

  Finally, the AI Act sets out several essential coordination points: (i) it does not affect, for example, the provisions on the liability of intermediary service providers under the Digital Services Act; (ii) it applies without prejudice to EU rules on consumer protection and product safety; and (iii) it also recalls that EU law on personal data and the confidentiality of communications remains applicable and that the AI Act does not affect those instruments.

7. NATIONAL IMPLEMENTATION OF PARAMOUNT IMPORTANCE

Even though the AI Act, as a regulation, is directly applicable, its operational implementation nonetheless requires national arrangements, in particular in terms of governance, market surveillance, inter-authority coordination and, where applicable, sanctions.

In Luxembourg, draft bill No. 8476 (**BILL 8476**) provides for the designation of a single point of contact and, in that context, proposes to entrust this role to the National Commission for Data Protection (**CNPD**), in line with the mechanism established by the AI Act.

BILL 8476 justifies this choice on grounds of institutional coherence and administrative efficiency: the CNPD is presented as the authority best placed to ensure centralised coordination, given the plurality of authorities that may be competent depending on the cases and the sectors concerned.

Lastly, in an “innovation/compliance” logic, the AI Act provides for the establishment of artificial intelligence regulatory sandboxes, i.e. controlled environments, supervised by the competent authorities, enabling the testing of innovative artificial intelligence systems for a limited period before they are placed on the market or put into service, on the basis of a testing plan agreed with the competent authority.

BILL 8476 provides that the CNPD shall establish “*at least one artificial intelligence regulatory sandbox, in accordance with the arrangements set out in Chapter VI of the AI Act, no later than 2 August 2026*.” In practical terms, the idea is to offer companies a framework in which they can test and fine-tune an artificial intelligence system under supervision, so as to identify the applicable requirements at an early stage and reduce legal uncertainty before deploying it at scale.

8. CONCLUSION

The AI Act is not just another piece of legislation: it introduces a new analytical framework for businesses, in which compliance is built not around an “AI” label, but around roles, risk levels and traceability requirements. It is precisely this architecture that makes the topic both unavoidable and, often, disconcerting at first glance.

The good news is that there is a method. In the next instalment, we will take a resolutely practical approach: where to start, which internal questions to ask, which points to address contractually, and how to anticipate situations in which an actor may, without intending to, move into a more onerous compliance regime. The objective is simple: to turn a dense text into a clear process, operational reflexes and clearly identified priorities.

* * * * * * * *

💡 Did you find this note helpful? Are you interested in AI and its implementation within businesses? Stay tuned: further publications will follow, to address AI and the AI Act in a simple and practical way.

For any questions or assistance, please do not hesitate to contact our partner **Pierre-Alexandre Degehet** (pierre-alexandre.degehet@kleyrgrasso.com).

Pierre-Alexandre DEGEHET
Partner

T +352 227 330 – 738
E pierre-alexandre.degehet@kleyrgrasso.com
www.kleyrgrasso.com

KLEYR_GRASSO
7 rue des Primeurs
L-2361 Strassen (Luxembourg)