

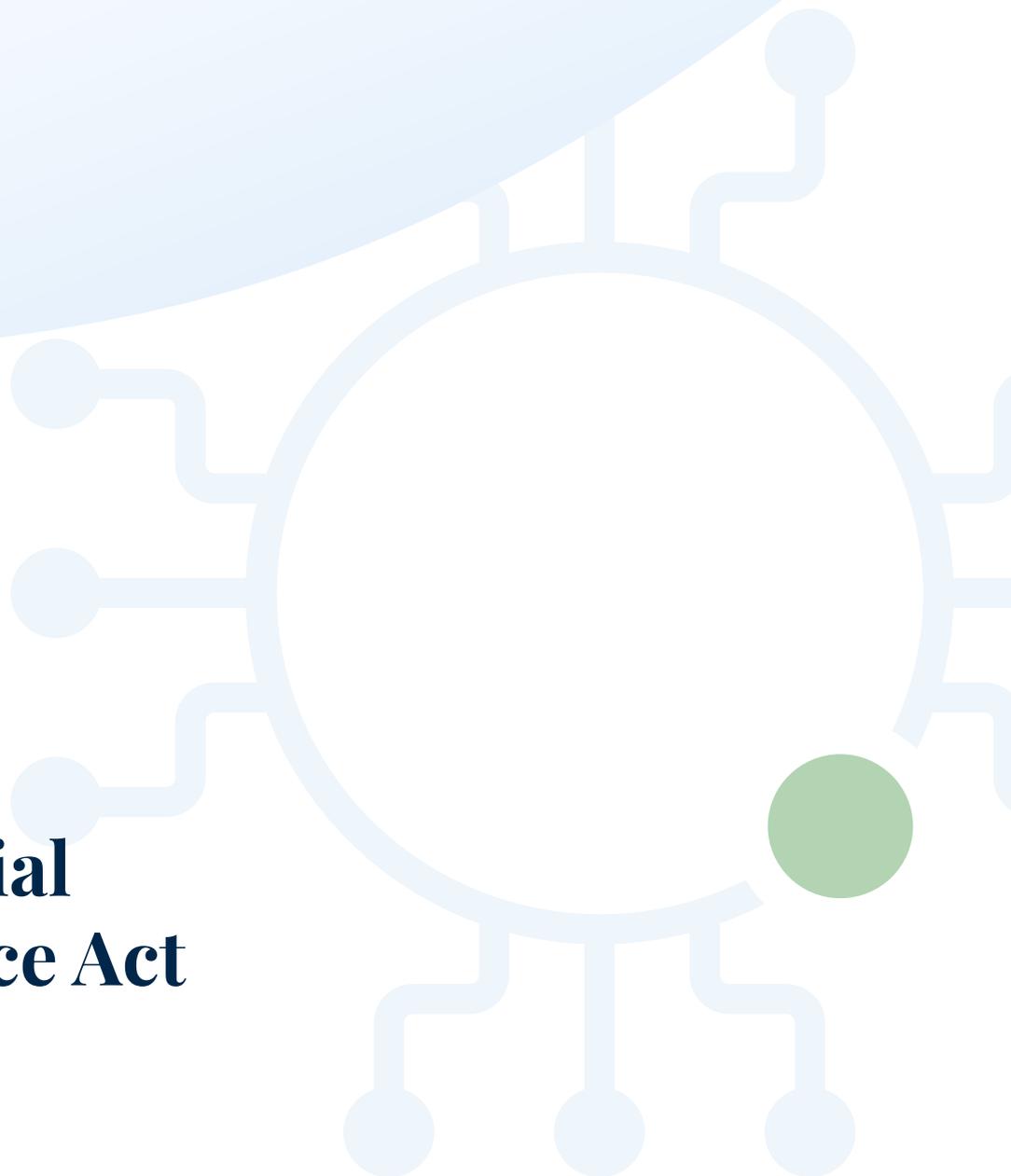


ERT

Expert Paper

EU Artificial Intelligence Act

March 2023



Introduction

The adoption of Artificial intelligence (AI) and data-driven tools will be a core driver of productivity and economic growth in Europe over the coming years. These tools will also play a significant role in addressing critical societal challenges brought to the forefront in the context of the COVID-19 pandemic and the climate crisis. The recent advances related to Generative AI have once again highlighted the remarkable potential of AI technologies, including for industrial use cases.

However, Europe currently lags behind its main competitors as concerns investments in AI (venture capital investments in AI in 2020: \$3.5 billion in the EU, \$19.8 billion in China, \$45.2 billion in the U.S.)¹. The McKinsey Global Institute states that “if Europe on average develops and diffuses AI according to its current assets and digital position relative to the world, it could add some €2.7 trillion, or 20 percent, to its combined economic output by 2030. If Europe were to catch up with the US AI frontier, a total of €3.6 trillion could be added to collective GDP in this period”²

Europe can leverage its technological capacity and strong industrial base with a high-quality digital infrastructure and a regulatory framework based on its fundamental values to become a global leader in AI and data-driven innovation. A coherent EU policy framework for AI has the potential to establish a Single Market for AI systems, to ensure legal certainty for AI providers and users, and to address legitimate public concerns around AI.

The Digital Transformation Working Group of the European Round Table for Industry (hereafter ‘ERT’) has assessed the European Commission’s proposal laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and welcomes its vision of creating trustworthy AI systems for Europe built around a human-centric and risk-based approach.³

At this stage of the legislative process, the following issues need to be addressed in the AI Act as a priority:

1. **Prevent unnecessary burdensome obligations** that could hamper AI adoption and innovation in Europe and **focus on regulating high-risk AI**. Refining the scope and concentrating on AI systems that pose a genuine risk to EU citizens in terms of health, safety or fundamental rights will be key to ensuring proportionality and legal certainty
2. **Establish a clear and fair allocation of responsibilities in the context of AI systems and their specific application**. It is important to appropriately differentiate between the different roles of providers and users as outlined in Article 23a of the Council General Approach. Providers and users must work together and exchange or share the necessary documentation and information to enable both of them to ensure compliance with the AI Act.
3. **Prevent any overlaps and competing obligations** between the AI Act and existing or future legislation in the EU. The AI Act should complement sectoral legislation without creating an accumulation of processes, obligations, and penalties. It is equally important for the EU to **foster global regulatory cooperation on AI** to avoid divergent approaches to AI governance and set global standards based on shared values.

¹ ERT Benchmarking Report 2022 <https://ert.eu/wp-content/uploads/2022/06/ERT-Benchmarking-Report-2022-LR.pdf>

² Tackling Europe’s gap in digital and AI, McKinsey Global Institute, February 2019 <https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-europes-gap-in-digital-and-ai#>

³ See also ERT’s Expert Paper on Artificial Intelligence, March 2021 <https://ert.eu/documents/ert-expert-paper-on-artificial-intelligence/>

ERT Recommendations on the AI Act

ERT would like to highlight the following priorities that EU policymakers should consider to set a regulatory framework that allows Europe to become a global leader in AI and data-driven innovation based on its fundamental values.

1. Prevent unnecessary burdensome obligations and focus on regulating a narrow scope of high-risk AI

Article 3 & Annex I

- **The definition of AI** goes beyond what is commonly considered AI technology. Including conventional algorithms or statistical methods in the scope will lead to significant constraints for companies in Europe to continue the use of those methods and innovate in the future. A more precise and “narrow” definition is needed, and should notably delete references to “Statistical approaches, Bayesian estimation, search and optimisation methods” all of which are quite simple and used virtually in all aspects of digital technology. In that sense, we welcome the adjustments made by the Council in its General Approach.
- The definition of AI systems should only cover software that is genuinely intelligent, more complex and has the ability to learn and infers how to achieve human-defined intended purposes by producing system-based-generated outputs (decisions, recommendations, content) which influence the environments they interact with.
- The high-risk category of “**access to and enjoyment of essential private services and public services and benefits**” should be narrowed down to concrete use cases.
- Situations where all AI systems for a given **high-risk sector** would be considered de facto high-risk must be avoided. The same is true for **prohibited AI systems** (Article 5): horizontal or fully blanket bans of certain AI applications (proposed via amendment proposals from several MEPs) may be counterproductive as they would not take into account current useful and safe uses (and potential future uses). An example is the early detection of emotions like aggression and stress on trams or trains that can prevent situations to escalate by using an edge-cloud AI application that would be forbidden in Europe under the AI Act.
- The classification of all applications as **high-risk in areas such as critical infrastructures, or employment and education** does not recognise the need to differentiate between applications according to the actual risks they pose to fundamental rights. We recommend restricting explicitly the scope in Annex III to the listed high-risk applications whose malfunctioning would directly harm people (e.g. for human health or human rights), and without final human decision-making (not all automated filtering of CVs is per se high-risk). Against this background, we welcome the 2-layer proposal in the Council's General Approach.
- The degree of **human oversight** should be adapted to the specific risks, the level of automation, and the context and intended use of the AI system to avoid hindering automated processes.

Annex III

- We advise considering AI in Annex III only as high-risk when **health, safety and fundamental rights of citizens** are at direct risk.
- The concept of **bias** should be clarified by using the more precise term “unwanted and harmful bias”.
- The definition of **remote biometric identification systems** needs to be further clarified as not all remote biometric identification systems in all contexts pose a risk to the fundamental rights and safety of individuals.
- We welcome the overall aim of the Council's General Approach to **clarify the scenarios in which AI systems designated in Annex III are viewed as being high-risk** and subject to additional compliance obligations. It is indeed critical to assess “the significance of the output of the AI system in respect of the relevant action or decision to be taken”. However, unless further clarified, the current wording of Art. 6.3 may have the same effect as the original draft: any AI system within the categories listed in Annex III that has any impact on human decision-making may be viewed as an inherently high-risk AI system.

- The use of an AI system should only be considered as high risk, when the **output of the system significantly determines what a person does or decides**, thereby limiting the individual's decision-making power. If there is adequate human involvement and oversight when an AI system is used, this is sufficient to avoid significant risks to health, safety, and fundamental rights. The term 'purely accessory' does not sufficiently reflect the influence of the output of the AI system on human decision-making. (See proposed amendment in the annex).
- On this aspect, we welcome the amended Recital 34 as proposed by the Council General Approach which notably clarifies **the concept of safety component**.
- Requirements on **robustness and accuracy** should be reasonable and based on the particular context and high-risk use case. Exploratory attacks, which can be aimed at revealing training data should be included.
- The process of **revision and extension** of the high-risk AI systems list (Annex III) should be further clarified for the sake of legal certainty. The process of periodically reviewing the list of high-risk AI systems should be clear, transparent, based on evidence and take place in consultation with involved stakeholders.

2. Establish a clear and fair allocation of responsibilities in the context of AI systems and their specific application

- The **responsibilities of the various actors**, including providers and users, should be appropriately allocated and tailored as per their respective competencies, as outlined in Article 23a of the Council General Approach. Providers and users must work together and exchange or share the necessary documentation and information to enable both of them to ensure compliance with the AI Act.
- **The Regulation should not detail specific obligations for providers of General Purpose AI (GPAI)**, and neither should the Regulation exempt such service providers. In our view, this debate has become a distraction from the many real and live issues which still need to be settled to arrive at a stable and coherent legal text (for example the overall definition of AI, high-risk categorisation, and governance mechanisms).

- We ask therefore that legislators remove all reference to GPAI in the text, considering that all AI systems are by definition general until they are applied to a specific purpose/function. Crucially, the Regulation needs to be based upon a definition of AI which is broad enough to encompass all variants and iterations of this technology, alongside a categorisation of high-risk AI which is narrow and precise enough to ensure that only those AI systems which pose a genuine risk to safety and fundamental rights of EU citizens are subject to additional ex-ante regulatory obligations and conformity assessment processes.

3. Prevent any overlaps and competing obligations in the EU and foster global regulatory cooperation on AI

It is key to **avoid inconsistencies** with other existing legislations and to define proportionate measures. The AI Regulation should complement sectoral legislation without creating an accumulation of processes, obligations, and penalties.

- We recommend streamlining **notification processes** at the EU level as various legislations require notification of incidents to different authorities under different thresholds.
- The **record-keeping requirement** should be based on the necessity and proportionality principle and be consistent with the GDPR. The proposal is questionable on several aspects including the requirement to keep technical documentation for over 10 years, including pictures, or record keeping of logs.
- Under the **transparency and provision of information requirements**, it will be important to clarify which information will be shared with which actors and for what purposes, while considering those scenarios that equally may prove impossible to provide such information or involve a disproportionate effort.
- Any **unrealistic absolute requirements** should be avoided, like data sets that need to be free of errors and complete.
- We recommend making use of already existing **quality management systems**, such as those defined by ISO 9001, instead of setting up a separate, dedicated AI quality management system.

- There is no need to deviate from existing **New Legislative Framework (NLF) conformity assessment procedures**, which are widely established in industry. We, therefore, do not support a mandatory registration of certain AI systems. In-house conformity assessment bodies should be allowed to assess the conformity of AI systems/applications of conformity assessment. The NLF already provides for the possibility to use in-house bodies for the performance of conformity assessment. Indeed, third-party conformity assessments should be limited to AI high-risk systems defined in Article 6.1. and those listed in Annex III to avoid its widespread promotion. In this context, we welcome the latest proposal on Recital 5a from the Council's General Approach: The AI Act should be in line with the New Legislative Framework Approach and be complementary to existing EU law, and not override any existing rights and remedies for consumers and others, including for compensation of possible damages.
- **Safety component of a product or system:** the definition in the proposed AI Act is not consistent with the same definition proposed in other legislations, the Machinery Regulation among others. For consistency and clarity, it is important to ensure that the definition is the same across the EU. The current definition of a "safety component" in the AI Act lacks a significant part of the definition in the draft Machinery Regulation that would make the text not only consistent but provide further certainty and predictability to the AI Act.
- We want to emphasise the importance of regulating with the function, not the AI system, in mind. We welcome the reference to update existing regulations, as exemplified with vehicle Type Approval, instead of regulating specific functions in general terms in the AI Act. To **avoid duplicating existing and new regulations**, it is essential that technical requirements are integrated into existing regulations and established industry standards, where the link to the high-risk systems should be defined.
- The definition of the **penalty regime** for non-compliance under this Regulation should be clearly delimited to avoid the risk of double penalties for companies in addition to the GDPR and other regulations. The fundamental principles under the GDPR should be applied for the development/use of AI systems as far as personal data protection is concerned.
- It is important to ensure **consistency between the AI Act and the AI Liability Directive**.
- **Cybersecurity requirements** should be in alignment with existing rules such as the NIS Directive, and the new NIS2 Directive.
- **Fostering closer cooperation with international partners:** Global regulatory cooperation on AI is vital to avoid divergent approaches to AI governance and to set global standards based on shared values. It should be a priority for the EU-US Trade & Technology Council (TTC) as well as in the Council of Europe, G7, G20 and OECD.

Conclusions

We are convinced that increased use of AI and data-driven technology is a necessary precondition for establishing a resilient European digital economy and society. We, therefore, welcome measures to boost the development and usage of AI, giving equal attention to the competitive promise as to the ethical dimension.

A harmonised and proportionate policy framework will be key to establishing a Single Market for AI products and services, providing legal certainty for AI developers and users and building consumers' trust in the technology across Europe. The AI Act should pursue and promote the competitiveness of European businesses and avoid putting in place regulatory obligations that could stymie AI adoption in Europe and hamper the innovation of European firms. Indeed, it must be part of a digital vision which allows sovereignty, competitive advantages for European companies, and better protection and services for European citizens and consumers.

Industry stands ready to support this effort. Public-private cooperation is vital, and the envisaged European AI Board should include industry representatives on an equal footing with public stakeholders.

Now is the time for the European Union to position itself strongly. It must reflect on its strengths and enact a long-term, fair, and holistic AI policy for the future.

ANNEX:

Suggested Amendment:

Article 6.3 (new)

AI systems referred to in Annex III shall be considered high-risk if the output of the system significantly determines the relevant action or decision to be taken and is not therefore likely to lead to a significant risk to the health, safety, or fundamental rights.

In order to ensure uniform conditions for the implementation of this Regulation, the Commission shall, no later than one year after the entry into force of this Regulation, adopt implementing acts to specify the circumstances where the output of AI systems referred to in Annex III would significantly determine the relevant action or decision to be taken. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74, paragraph 2.



The European Round Table for Industry (ERT) is a forum that brings together around 60 Chief Executives and Chairs of major multinational companies of European parentage, covering a wide range of industrial and technological sectors. ERT strives for a strong, open and competitive Europe as a driver for inclusive growth and sustainable prosperity. Companies of ERT Members are situated throughout Europe, with combined revenues exceeding €2 trillion, providing around 5 million direct jobs worldwide - of which half are in Europe - and sustaining millions of indirect jobs. They invest more than €60 billion annually in R&D, largely in Europe.

This Expert Paper has been prepared by the ERT Working Group on Digital Transformation.

More info and previous papers on: <https://ert.eu/focus-areas/digital-economy/>

Contact: Hanno Woelm (hanno.woelm@ert.eu)

+32 2 534 31 00
contact@ert.eu

 [@ert_eu](https://twitter.com/ert_eu)
www.ert.eu

Boulevard Brand Whitlocklaan 165
1200 Brussels, Belgium

© ERT 2023