AmCham Romania
www.amcham.ro
amcham@amcham.ro

24 April 2023

POSITION PAPER

on the working version of the European Commission Proposal for the Artificial Intelligence Act (AI Act)

INTRODUCTION

AmCham Romania supports the efforts at the level of the European Union (EU) aimed at the regulation of Artificial Intelligence (AI) through an approach entailing a robust and comprehensive framework that encourages the EU to become a hub for innovation, trust and excellence in research and development of new technologies.

The European Commission carried out an extensive public consultation process before the publication of the *Proposal for a Regulation laying down harmonised rules on artificial intelligence*[1] (the AI Act or the Regulation). The AI Act constitutes a core part of the EU digital single market strategy with the stated purpose to improve the functioning of the internal market. Overall, the AI Act aims to foster innovation and growth in the EU's AI sector while also ensuring that AI is developed and used in a way that is safe and respects fundamental rights. In December 2022, the EU Council adopted its common position[2] ('general approach') on the AI Act. Its aim is to ensure that AI systems placed on the EU market and used in the Union are safe and respect the existing law on fundamental rights and Union values.

The present document outlines the feedback of AmCham members on the current working version of the proposed regulation, having in mind a practical approach for organisations to conform to the EU regulations with regards to artificial intelligence. In doing so, the aim is to outline how to properly employ data effectively to achieve the desired outcome while managing the autonomy of AI systems and, overall, **strike a balance between the achieving core regulatory goals and maintaining an environment that is conducive to more innovation**. When regulating the use of AI, it is important thus to keep in mind that the cost of regulation should not become so high that it prevents safer and better products and services from reaching the market.

We believe that continuous feedback during the legislative procedure from all stakeholders is an essential part in laying down, to the extent possible, a new sound piece of legislation. Therefore, we are confident that the following observations might provide useful insights for EU institutions towards **shaping and improving the Regulation during the legislative procedure, especially in light of the upcoming votes in the European Parliament and the following trialogues**.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206
[2] https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf

CLEAR AND PRECISE DEFINITION OF AI SYSTEMS

We welcome the fact that, through its position, the Council improved and narrowed down the definition of AI systems, to provide clearer criteria for differentiating AI from simpler software systems and that should apply to systems developed through machine learning approaches and logic and knowledge-based approaches.

As stated previously, a **clear and precise definition** should constitute an essential aim of the current regulatory effort, in order to avoid legal uncertainty, over-regulation and thus facilitate the subsequent application and enforcement of the new piece of legislation at hand. A broad definition may excessively encompass general purpose tools that are used for the development of AI systems (software serving as building blocks) or may over-regulate, given the variety of tools we use in modern society, a great number of software which are not normally considered AI (for example, GPS systems). Such aspects could impact or hinder the benefits that AI may offer. For these reasons, **we support the adoption of a definition of AI that is aligned with international standards and that does not include non-AI tools**.

Also, the mentioned aspects herein have been a constant desideratum of the stakeholders involved in the consultative process, as the European Commission highlighted in the Explanatory Memorandum which accompanies the Regulation.[3]

THE LIFEBLOOD OF AI: DATA

In simple terms, an AI System involves using computers to do things that traditionally require human intelligence. The AI System has the capacity to process large amounts of data in ways humans cannot. The further goal of AI Systems is to develop competences such as the recognition of patterns, decision-making and judgement, similar to those of humans.

Developing advanced AI and machine learning models for any AI System is challenging, as they require large quantities of data and the accurate labelling of that data in order to train their systems effectively. Even with the most cutting-edge generative AI systems, such as *chatGPT*, which utilises transformers and reinforcement learning, their performance is heavily influenced by the accuracy of the labelled data examples used for training. For example, building an AI system that can analyse patient ECG data and provide detailed reports to doctors and specialists would require establishing all data security and high-risk AI system requirements before the AI system can be built. In contrast, countries with less rigorous legislation outside of the EU will always have an advantage in building impactful AI systems as they have no boundaries to access data.

We suggest applying EU guidelines to ensure practical realisation and interpretation of the legislation, making public anonymised data digitally available for research and innovative businesses without compromising data privacy and security protection principles. This

[3] 3.1. Stakeholder consultation: […] *"Stakeholders mostly requested a narrow, clear and precise definition for AI."*

approach has already been proven to be very effective in accelerating research during the COVID-19 pandemic when data was made digitally available for collaboration. **Data privacy protection should be a fundamental principle,** rather than trying to impose the guidelines in an unpractical way by demanding that the data be free of errors. Moreover, it is well known, based on the experience of the industry, that error-free master data of business ERP systems do not exist. One should also consider that it is not possible to eliminate any biases in the underlying data due to technical limitations and cultural bias of people who implemented the data collection methods.

Not least, we understand that the requirement of users to "*fully understand the capacities and limitations of the AI system*" is an essential and reasonable one to ensure protection from the decision autonomy of an AI System. Yet, such requirement (Art. 14.4.(a) to put in place human oversight enabling an user to "*fully understand the capacities and limitations of the AI system*" is not possible to achieve in practice since a developer cannot guarantee what a user will understand.

GENERAL PURPOSE AI

The Council's position adds new provisions to account for the situations where AI systems can be used for different purposes **(general purpose AI – GPAI)** and where GPAI technology is subsequently integrated into another high-risk system. Certain requirements for high-risk AI systems would also apply to GPAI systems in such cases and an implementing act would specify how they should be applied for such GPAI systems, based on a detailed impact assessment.

While the initial draft of the European Commission did not mention the GPAI systems at all, we believe that **the current proposed approach on GPAI could undermine the high-risk based concept and could impose too burdensome and complex obligations on providers, regardless of the low risks associated with the system**. In particular,

- **Recital 60b** requiring *"independent oversight by independent experts for GPAI providers, tasks them with developing GPAI requirements that are "broadly applicable... address risks specific to GPAI... can be coherently implemented... includes risk management, analysis and testing, etc."* & **Art. 58 (cb)** providing for *"particular oversight and monitoring of general purpose AI systems as well as AI systems that make use of such AI models and best practices for self-governance"* create very heavy and disproportionate regulatory obligations and oversight, the latter which would apply to all GPAI and therefore deviating from the risk-based approach, compared to the Commission's original proposal. So does **Art. 28.2,** when it comes to the last paragraph about API access, that is not technology neutral and might prohibit access models such as those ChatGPT currently use. It seems to only allow GPAI access via API if the provider fulfils all the disclosure obligations for high-risk AI which, once again, deviates from the risk-based approach;
- The suggested **Art. 28b** is very concerning for several reasons, primarily because it creates a separate set of obligations for all GPAI regardless of how they are used and the level of

risk. The proposal does not distinguish the obligations along the AI value chain, nor it provides any clarity on whether this would apply to all general purpose AI, or to specific use-cases. This is inconsistent with a risk-based approach to AI and would include an enormous amount of non high-risk AI systems and tools in the scope of the Act. All these obligations would also be duplicated if a GPAI were to be placed in one of the Annex III uses. Our recommendation would be to delete this article, and instead work on a reformed version of Art. 52, where the concerns that are related to GPAI (or specifically generative systems) can be properly addressed both from a transparency perspective, and from a communication and information perspective. Overall, **any obligations should be limited to general purpose AI systems that are used as high risk systems**. More specifically to the obligations for GPAI in Art. 28b:

- The requirement to comply with "use-agnostic" requirements is impossible to comply with since, along the obligations of Art. 9, it would request a GPAI developer to assess risks for every possible use. GPAI developers are not the entity best placed to assess risks in uses and sectors they can not know in advance. A risk assessment and management system based on very limited information would not be efficient, effective and technically possible;
- Several requirements – e.g. for data governance and a Quality Management System (QMS) – do not consider the very diverse set of GPAI applications and would be impossible to comply with in some cases. Not all developers have access to the datasets used for training, nor are all relations based on a binary developer-deployer dynamic. It is difficult to document/imagine all of the limitations of a general tool or system, or to test completely for bias when the end use is not yet known. Requiring all developers of GPAI to establish a QMS would be a very significant and disproportionate obligation, especially if it were to continue downstream the value chain regardless of the degree of control of the various developers and deployers. This is also technically unfeasible since developers cannot predict all possible risks related to use;
- The requirement to have GPAI assessed by independent experts is disproportionate, and not in line with the rest of the AI Act. GPAI would receive a more stringent treatment than high-risk AI, which would remain instead under self-assessment. This also poses the question of resources, both for developers and for the AI Office and the European Commission;
- The obligation to register GPAIs in an EU database prior to being put on the market again puts these at the same level as high-risk systems. Such an provision is not consistent with the risk-based approach.

- Not least, several articles do not properly take into account the very **diverse AI value chain**. For instance, **Recital 60a** neglects the fact that the downstream operator has total control over how to deploy the system and specify their requirements to providers. We cannot imagine any situation where a downstream operator "controls" an AI system's development upstream. In addition, when it comes to **Art. 28.3**, the addition of the possibility for the Commission to draft model contractual language is concerning since these model contracts could limit flexibility regarding the allocation of responsibility and liability with deployers.

Therefore, we suggest focusing on the initial proposal of the Commission and not regulating the general purpose AI as such, as it might become too difficult to implement such provisions that are not clear enough and that could lead to undesired outcomes in practice.

Provisions such as **Recital 60a** noting that "*AI systems developed for a limited set of applications that cannot be adapted for a wide range of tasks such as components, modules, or simple multi-purpose AI systems should not be considered general purpose AI systems for the purposes of this Regulation*." are particularly welcome as they make a **useful distinction between tools and systems**. Not least, the start-up ecosystem also raised concerns on a vast number of their applications being considered as GPAI and therefore they will be subject to strict scrutiny and obligations which can impede their activity.

HIGH-RISK AI SYSTEMS

We acknowledge the improvements made by the Council in clarifying and adjusting the high-risk AI systems classification, in order to make the application more technically feasible and less burdensome for stakeholders to comply with, as it is stated for the quality of data, or when it comes to the obligations of small and medium-sized enterprises (SMEs).

However, we believe that the text still remains applicable to a wide range of high-risk systems, which are already regulated by other product safety laws. The Annex III provides an overly broad and vague interpretation and no clear methodology for defining a high-risk systems and could lead to legal uncertainty that could subsequently result in stifling innovation and making enforcement very difficult, whereas the oversight authorities will have a difficult task in assessing the potential misuses of AI applications.

The concept of high-risk AI system is important given that regulated actors must interpret and apply it in determining whether they are subject to mandatory regulatory provisions. However, the list-based approach may consider some AI systems as being high-risk, irrespective of their specific use and of the fact that such use may not pose in all cases a risk to the health and safety or to fundamental rights. For example, classification of all human resources (HR) applications as high-risk does not recognize the need to differentiate between applications in the area of HR according to actual risks they pose.

In determining whether an AI system is high-risk, it might be more appropriate for the users to assess the risks following a case by case basis analysis and take industry-specific

mitigation techniques. In carrying out this assessment, it should be taken into account both the severity of potential harm and the likelihood that this harm will occur.

On the other hand, the concept of risk should also consider the benefits of the AI system and the losses that could arise from not adopting the AI system.

REQUIREMENTS FOR HIGH-RISK AI SYSTEMS AND STATE-OF-THE-ART STANDARD

While the AI Act contains certainly high-level goals, it is not clear that imposing substantive or outcomes-based compliance requirements is the best approach.

Specifically, some requirements for high-risk AI systems, such as the ones referred to in **Art. 10.3** seem rather generic ("*data sets must be relevant, representative [...] and complete*") or impossible to comply with ("*data must be free of errors*"). Also, the requirement to put in place human oversight that enables the user to "*fully understand the capacities and limitations of the AI system*" in Article 14.4.(a) is rather impossible to achieve in practice, since a developer cannot guarantee what a user will understand.

In addition, it is not clear how accuracy would be evaluated, or what the benchmark would be. Although those points are critical, it is equally important to recognize that there is no single, "correct" level of accuracy (for instance, accuracy levels for an AI system used to decide when to apply the brakes on an autonomous vehicle would be meaningfully different than that used to predict whether a consumer would prefer a green or blue blouse).

If the idea is indeed, as it seems from the text of the Act, that **compliance with the requirements must be done with state-of-the-art levels in mind**, as in "*consistent with industry standards*", then we believe the Regulation could be amended to further clarify this point.

We suggest better guidance by providing examples that can be put into practice. For example, practical requirements for data anonymisation could be set for the development of high-risk AI systems instead of creating unclear guidelines and measures for these high-risk AI systems. Protect the underlying data of high-risk AI systems and the affected individual's data will be protected without applying ambiguous controls to the AI system.

OBLIGATIONS OF PROVIDERS AND USERS

Given the complexity of the AI marketplace, especially the diversity of roles and responsibilities, the methodology for identification of the party holding "provider" or "user" responsibilities should be clarified with a complex, evolving AI ecosystem in mind, in order to avoid legal uncertainty.

The allocation of compliance responsibilities is particularly relevant when it comes to general purpose tools used for the development and training of AI systems. Therefore, we consider that the text of the Regulation must be more explicit in this regard.

We recommend to classify as providers users or other third-parties that train or otherwise modify a general purpose tool in such a way that it becomes a high-risk AI system. Also, the parties mentioned in Recital (60) that are urged to cooperate with providers and users should not be considered, by adding an express wording, providers for the purposes of the AI Act.

To be effective, **the Regulation should leave no uncertainty about which requirements apply to which actors and should ensure that responsibilities always fall on the actor that can most efficiently and effectively comply with them**.

SAFEGUARDING THE DECISION AUTONOMY OF AI SYSTEMS

Stringent criteria, rooted in practical applications, should be put in place to ensure protection from the potential decision autonomy of AI systems. Such criteria should include comprehensive monitoring of the system's ethical operations and implementation of proper safeguards to evaluate all possible protocols. This will ensure that **only safe and responsible AI systems are deployed for productive use.**

Operators and Providers of AI Systems should be able to provide auditable test cases which can be verified against the expected outcome. Thus, it will not be necessary to verify the underlying data that has been used for the development of the AI Systems, which is very difficult to verify, rather we see outcome-based testing as a practical way to ensure that the "capacities and limitations of the AI system" can be fully understood and ensure the necessary human oversight.

When it comes to productive high-risk AI systems, maintaining records of all outcomes is essential in order to ensure accurate, reliable, and trustworthy results. This serves two important purposes, namely continuous verification and regular human verification. Continuous verification is necessary to ensure that the AI system consistently produces the same accurate results and has not developed any systematic errors or biases.

Operators and Providers of high-risk AI Systems should be required to install proper verification procedures and keep records of all AI System transactions and outcomes. If an Operator and Provider cannot adhere to these criteria, they must ensure that a human manually approves all outcomes or decisions from a high-risk AI system to guarantee their validity.

To facilitate the development of cutting-edge innovation solutions without overburdening the process, record-keeping and verification procedures should be omitted for AI systems (e.g. research AI systems) which are not high-risk so long as data remains subject to privacy or security data protection measures.

SKILLS

Developing and nurturing competences and digital skills (both basic and specialized) among EU citizens will be crucial for stimulating the development of AI systems, promoting the uptake of AI technologies among both public and private sectors (especially SMEs), and finally boosting the Digital Economy and Society Index (DESI) indicators.

Furthermore, as lifelong learning becomes a necessity, mechanisms for assessing and validating the outcomes of non-formal education and informal learning will also be fundamental in supporting citizens in their career paths, while ensuring stability within the EU labor market.

ENCOURAGING INNOVATION

When regulating the use of AI, it is important to keep in mind that **the cost of regulation should not become so high that it prevents safer and better products and services from reaching the market**. In many cases, the use of AI—even in high-risk scenarios—may actually make products and services safer, better, or more accurate than their non-AI counterparts. Therefore, the EU needs to find the right balance in order to encourage development and deployment of AI within the single market.

We welcome the opportunity to introduce **regulatory sandboxes** that can be used by developers to test their products and systems in both unsupervised real-world testing and controlled environments. We understand that new provisions added by the Council are meant to allow even smaller companies to deploy such regulatory sandboxes by implementing supportive actions for such operators and providing limited and specified derogations. However, it is important to stress out the potential discrepancies between economic opportunities in different Member States and between the capabilities of private companies to properly test their systems before releasing them into the market. Thus, it is vital to put in place sufficient safeguards to ensure that every stakeholder could benefit from the advantages envisioned by introducing these regulatory sandboxes. We support that the self-assessment model of conformity will be key to encourage innovation, entrepreneurship and progress on research and development of new technologies.

FINAL RECOMMENDATIONS

Our final considerations when it comes to the regulation of AI are as follows:

- Establish a clear definition when defining an AI system, in order to avoid legal uncertainty and over-regulation;
- Set practical guidelines to make data available for research and innovative businesses;
- Apply EU guidelines while allowing practical realisation considerations of the legislation;
- Foster practical requirements for data anonymisation rather than creating unclear guidelines and measures for high-risk AI systems;
- Consider outcome-based testing as a practical way to ensure "capacities and limitations of the AI system" can be fully understood;
- Install proper verification procedures and keep records of all transactions for productive high-risk AI systems;

- For non-high-risk AI Systems record-keeping and verification procedures should be omitted as long as data remains subject to privacy or security data protection measures;
- Consider the provision of public anonymised data digitally available for research and innovative purposes pursued by businesses, without compromising data privacy and security protection principles.

The EU AI Act is a significant milestone in governing the responsible development and use of artificial intelligence. If adequately enacted, we believe our recommendations would create a framework in which applied AI could be developed to its full potential. This would help to realise major advances in health, automation, and a host of other sectors which could benefit from the use of AI-enabled technology.

These recommendations would also ensure that any AI system conforms to the AI Act's ethical principles. By encouraging a safe and law-abiding practice of AI technology, these suggested provisions could foster an environment conducive to more innovation while also providing a measure of assurance to the public that these systems comply with the set of rules established by the Act. Additionally, it may also lead to greater public trust in AI applications and pave the way for broader adoption and implementation of AI and other advanced automation technologies.